Secondary and Approximate Authorization Model and Its Applications to BLP and RBAC Policies

Konstantin (Kosta) Beznosov

Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
University of British Columbia, Canada

University of British Columbia

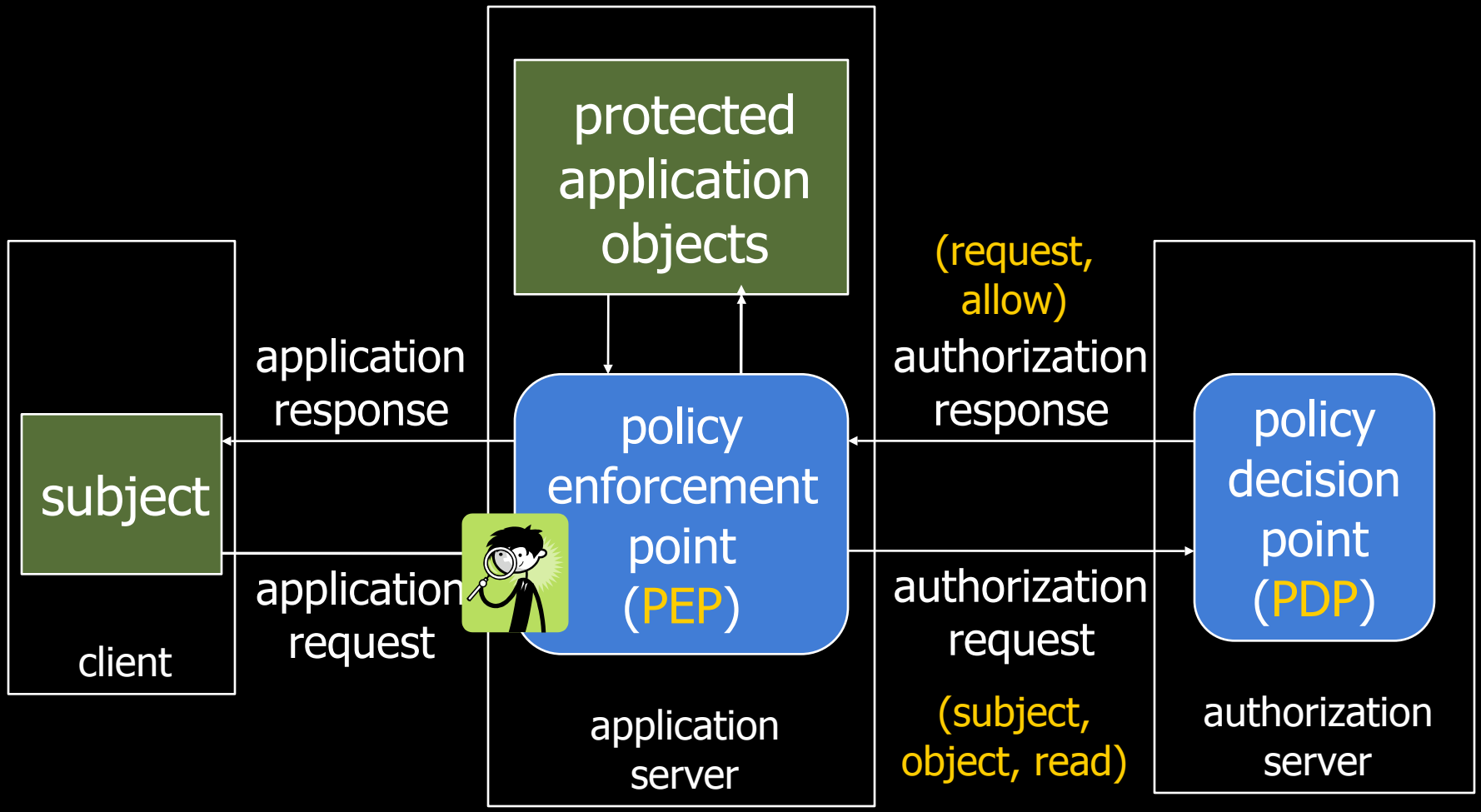
founded in 1908
ranked among the world top

- 40 institutes, by the *Shanghai Jiao Tong University, 2007*
- 27 universities, by *Newsweek* magazine in 2006
- 38 universities, by the *Times Higher Education Supplement* in 2005

departing assumptions

- processor resources virtually free
- commodity computing most cost-effective
- network bandwidth virtually unlimited
- human time/attention expensive

a typical authorization architecture



IBM Access Manager, Entrust GetAccess, CA SiteMinder, etc.

request-response paradigm

request-response paradigm

+ re-use of authorization logic
+ consistent policy enforcement
+ lower admin overhead

PEP

PEP

PEP

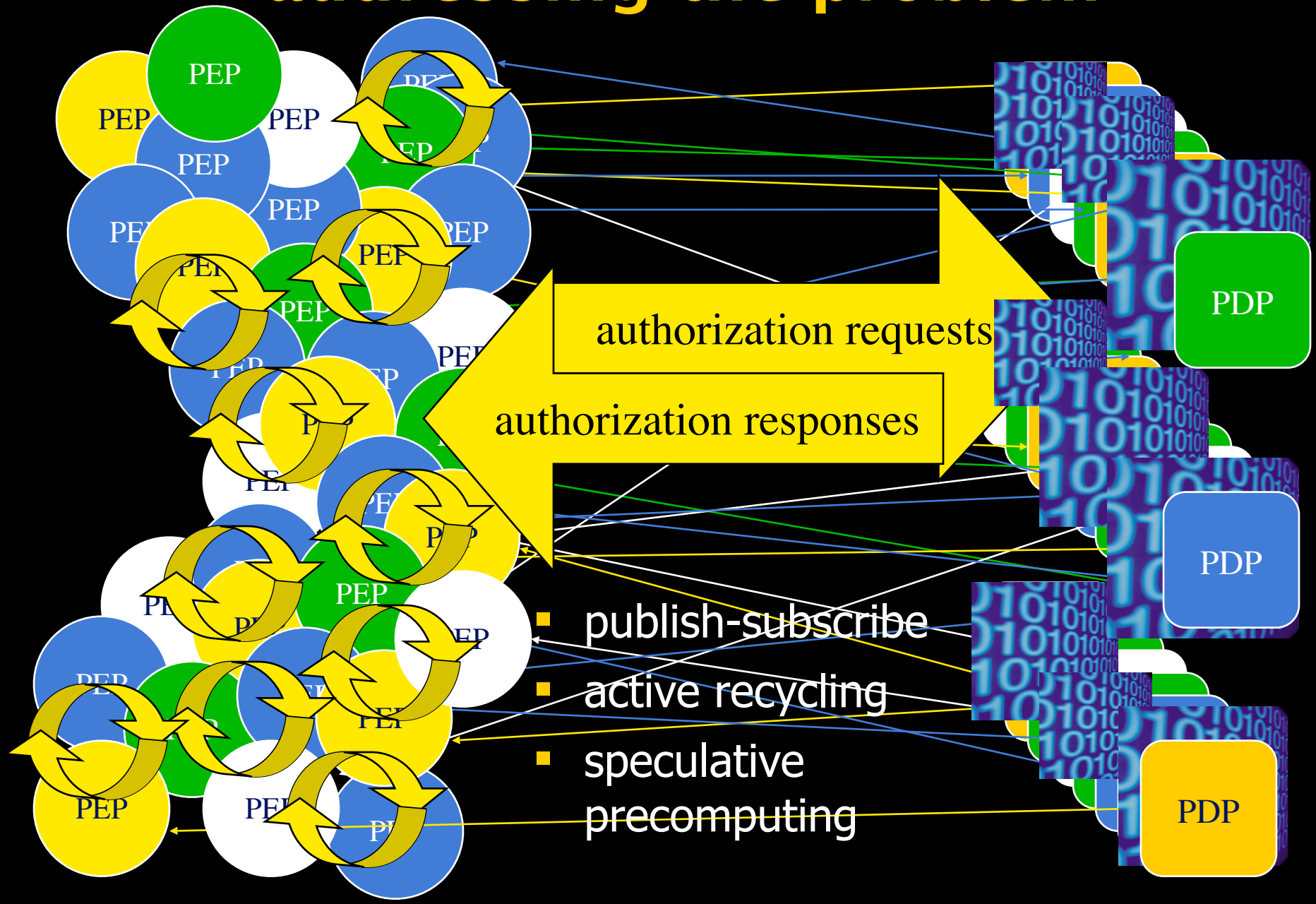
PDP

- reduced availability
- increased latency
- reduced scalability

existing approaches

- caching previous authorizations
  - + simple, inexpensive
  - + improves performance & availability
  - - serves only returning requests (precise recycling)
- generic fault-tolerance through replication/redundancy
  - + improve availability
  - - latency remains unchanged
  - - require specialized OS/middleware
  - - poorly scale on large populations

addressing the problem



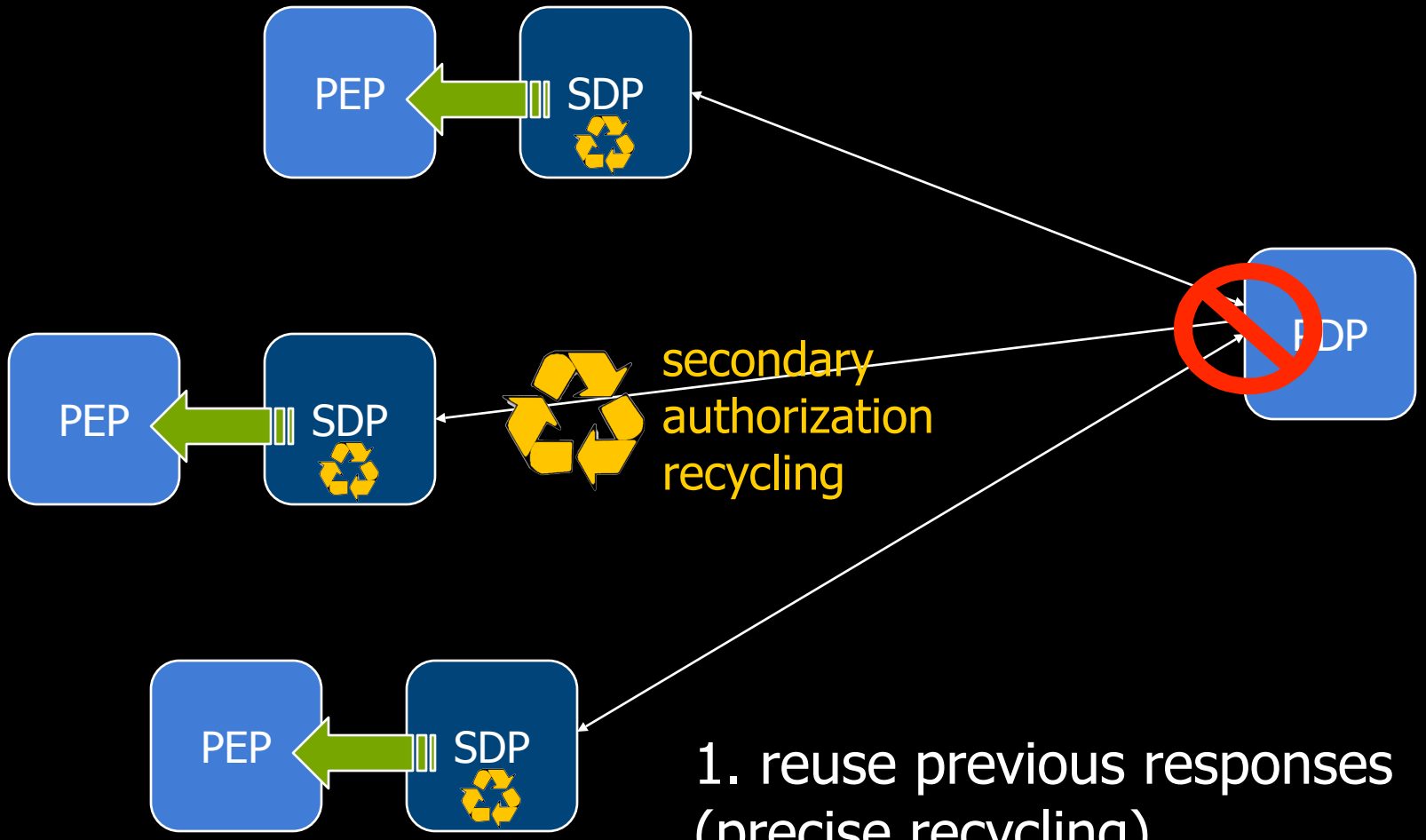
K. Beznosov, "Flooding and Recycling Authorizations" in Proceedings of New Security Paradigms Workshop (NSPW), 2005, Lake Arrowhead, CA, USA, 20-23 September 2005, pp. 67-72.

contributions

- concept and model for inferring new authorizations from previous responses: secondary and approximate authorization model (SAAM)
  - secondary decision point (SDP)
  - classified response space
- SAAM algorithms for BLP and RBAC
- distributed and cooperative SAAM

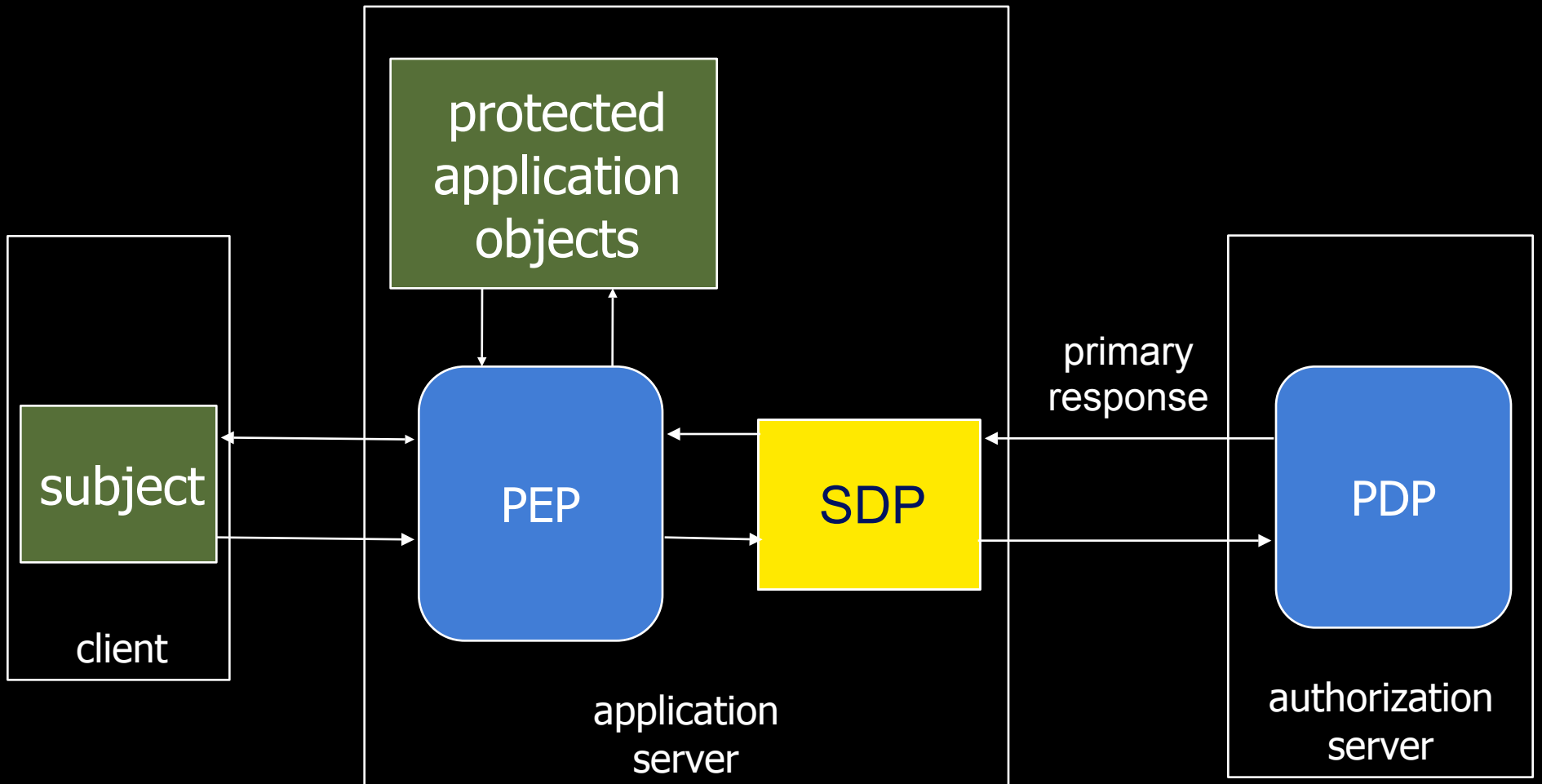
Secondary and Approximate Authorization Model (SAAM)

secondary decision point (SDP)

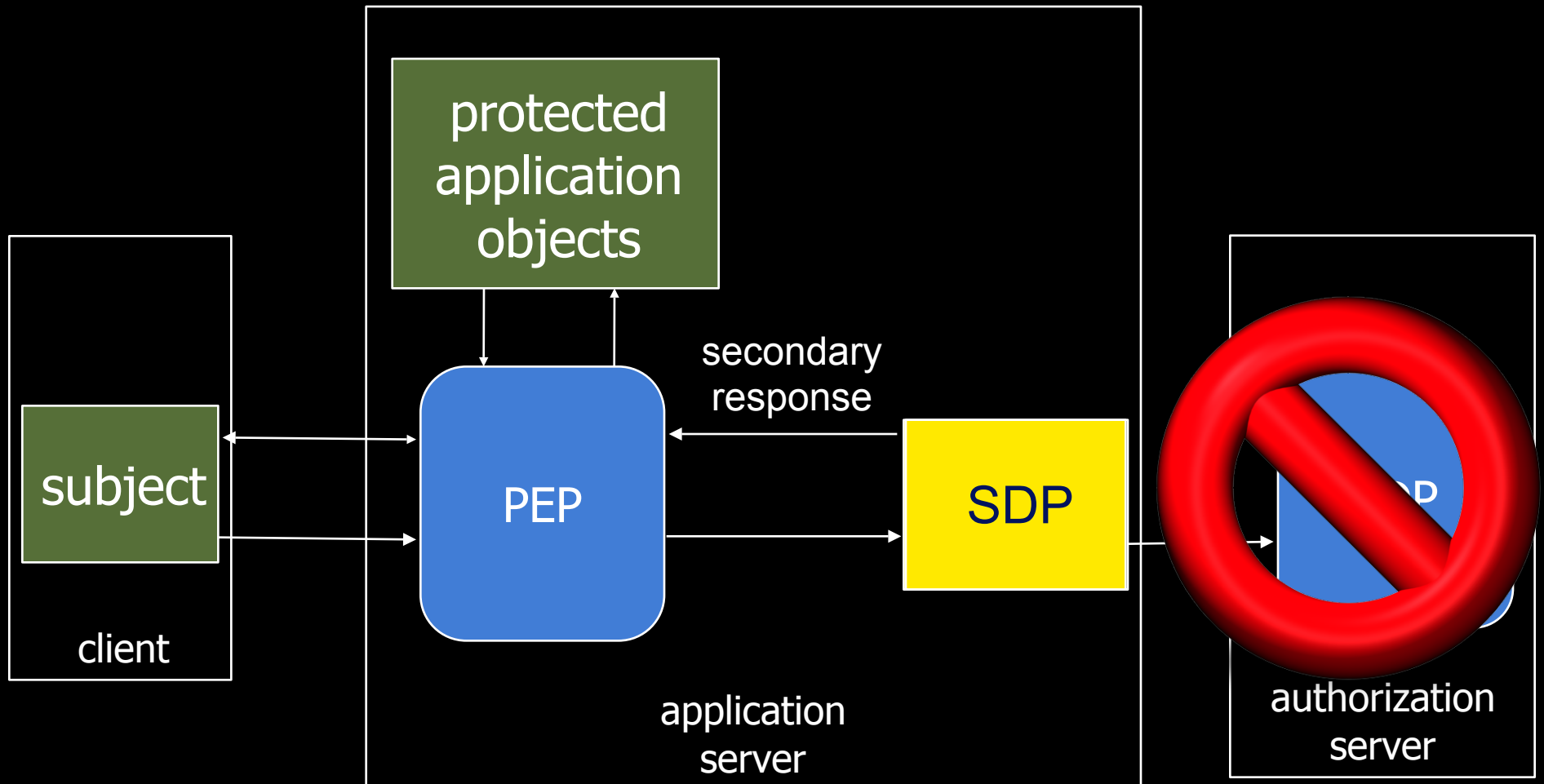


1. reuse previous responses (precise recycling)
2. infer approximate responses (approximate recycling)

what SDP does



what SDP does



SAAM basic elements

- request
  <subject, object, access right, context, request id>

  < s , o , a , c , i >
  <{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05-08-15"}, 10 >

- response
  <response id, request id, evidence, decision>

  < r, i, E , d >
  < 1, 10, [ ], allow >

authorization response types

<{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 10>

< 1, 10, [ ], allow > -- primary (from PDP) response

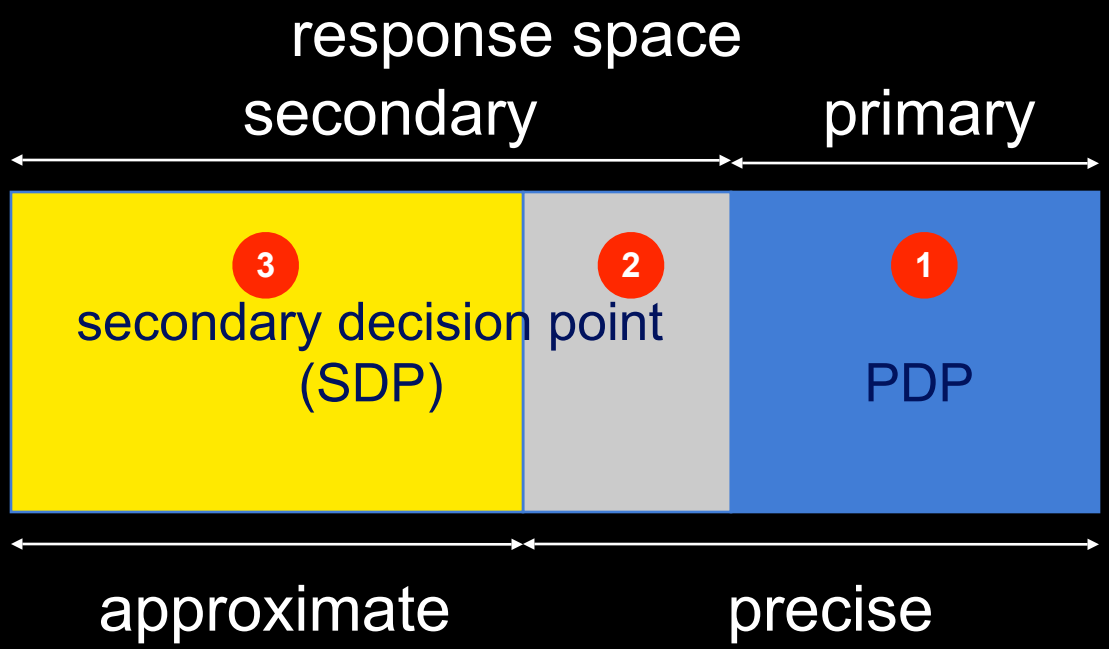
<{id="Bob", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 11>

< 2, 11, [1], allow > -- secondary and precise response

<{id="Alice", role="customer"}, {id="eB-23"}, view, {date="05.06.08"}, 12>

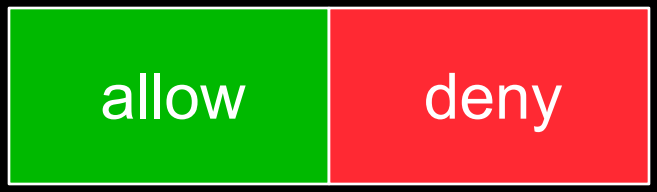
< 3, 12, [1], allow > -- secondary and approximate response

equivalent



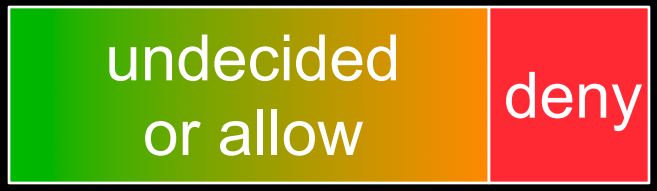
SDP Types

PDP



safe SDP

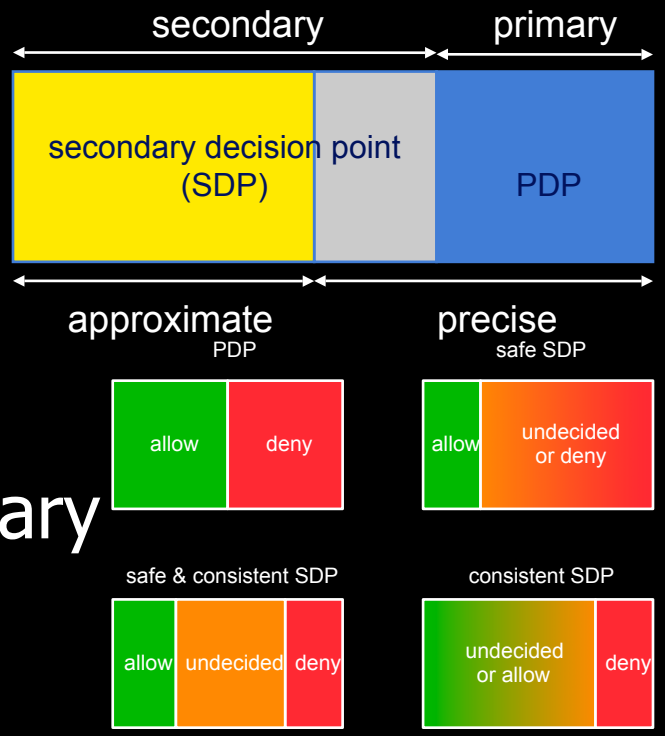
consistent SDP



safe & consistent SDP

SAAM summary

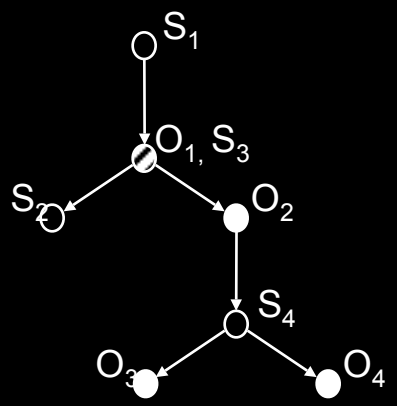
- basic elements
  - authorization requests <s, o, a, c, i>
  - authorization responses <r, i, E, d>
- responses can be
  - primary or secondary
  - precise or approximate
- secondary decision point
  - implemented at PEP
  - uses primary to compute secondary
  - can be safe and/or consistent



Application of SAAM to Bell LaPadula Policies

What's $SAAM_{BLP}$?

1. dominance graph (DG)

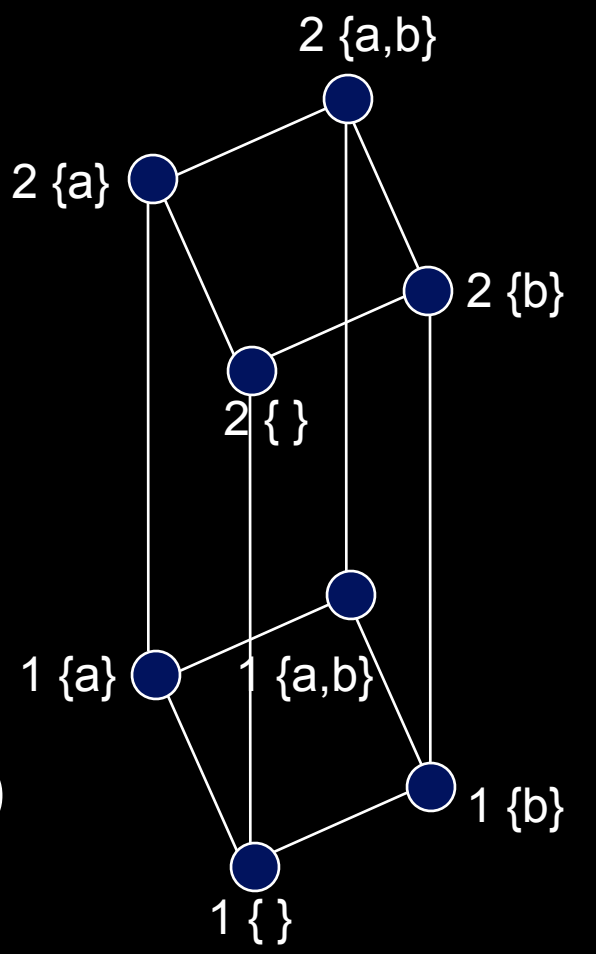


2. algorithms for SDP to
   - build DG from primary responses
   - compute secondary responses using DG

BLP refresher

- S : subjects, O : objects
- DAC
- L: lattice of security labels
- λ: S $\cup$ O $\rightarrow$ L

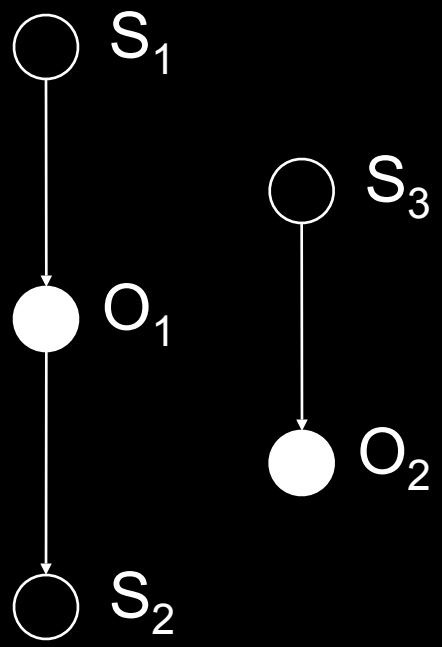
- ss-property, $*$-property:
  - (s, o, read) is allowed $\Rightarrow \lambda(o) \leq \lambda(s)$
  - (s, o, append) is allowed $\Rightarrow \lambda(o) \geq \lambda(s)$
  - (s, o, write) is allowed $\Rightarrow \lambda(o) = \lambda(s)$



dominance graph

allow

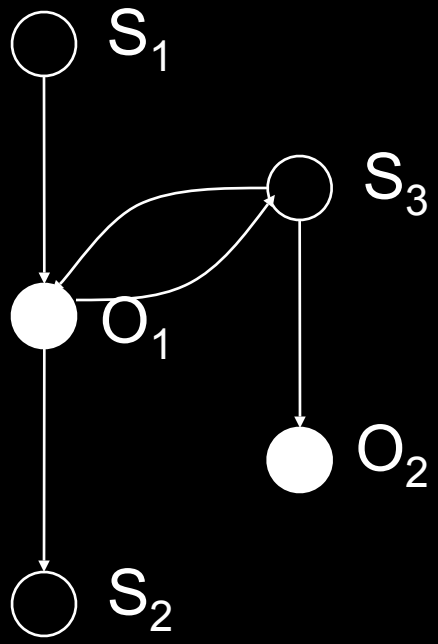
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)



dominance graph

allow

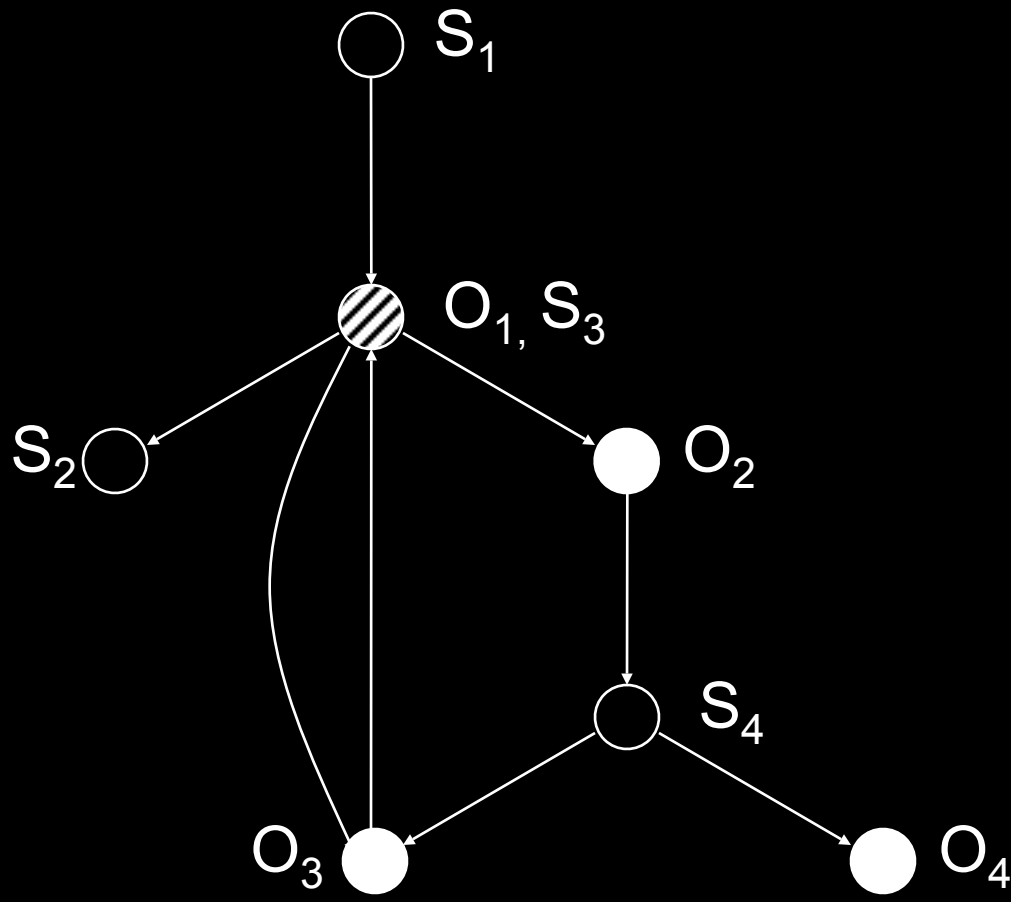
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)



dominance graph

allow

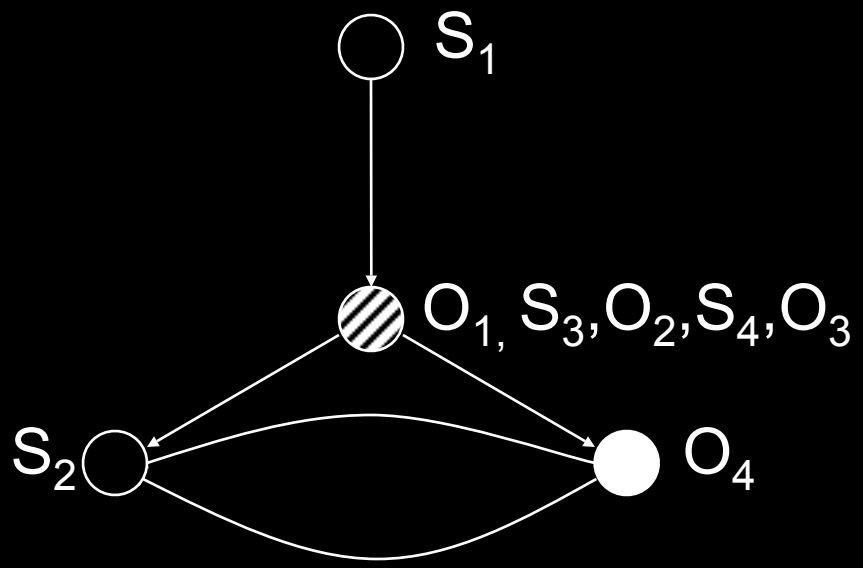
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)



dominance graph

allow

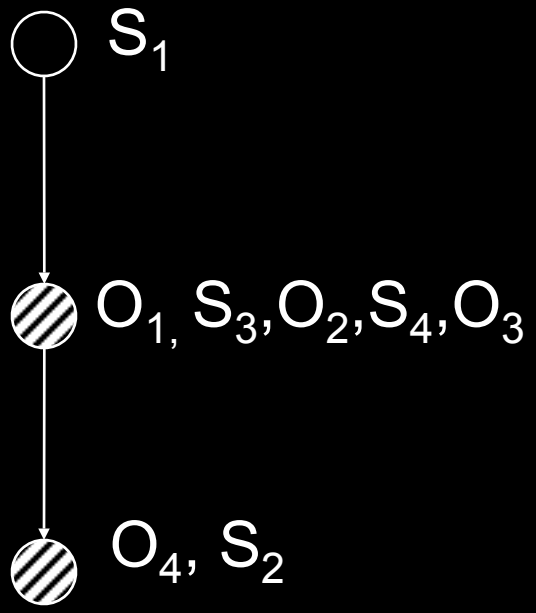
1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)
10. (s_2, o_4, write)



dominance graph

allow

1. (s_1, o_1, read)
2. (s_2, o_1, append)
3. (s_3, o_2, read)
4. (s_3, o_1, write)
5. (s_1, o_2, read)
6. (s_4, o_2, append)
7. (s_4, o_3, read)
8. (s_4, o_4, read)
9. (s_3, o_3, write)
10. (s_2, o_4, write)



SDP may allow:

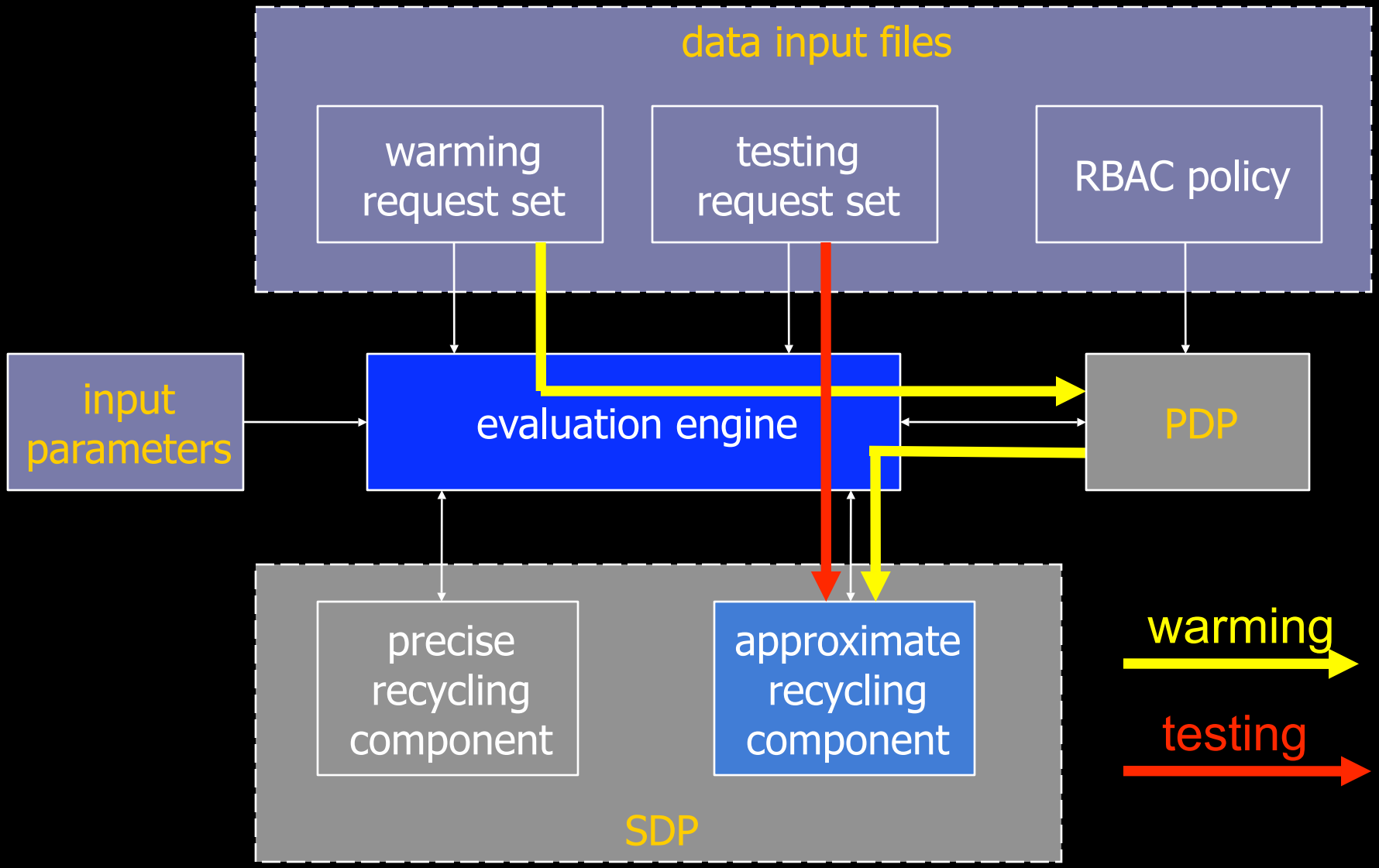
- (S_1, O_4, read)
- (S_4, O_1, write)
- (S_2, O_3, append)

SDP cannot decide:

- (S_2, O_3, read)
- (S_1, O_4, write)
- (S_1, O_4, append)

$SAAM_{BLP}$ evaluation

evaluation methodology

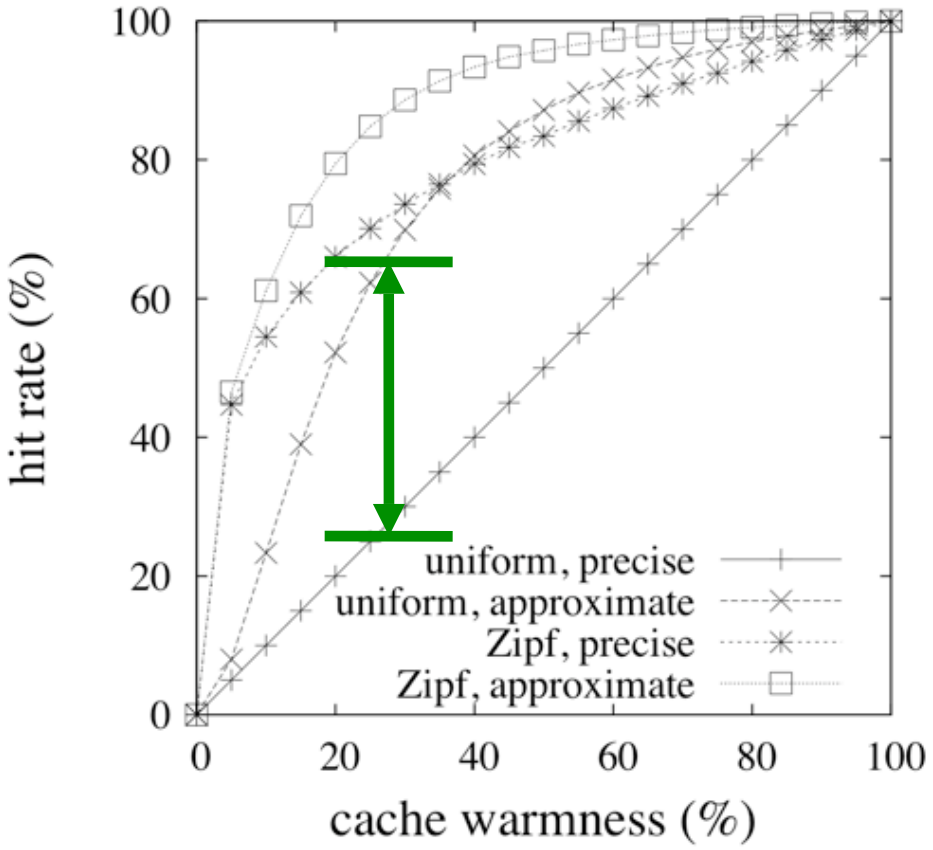


evaluation metrics

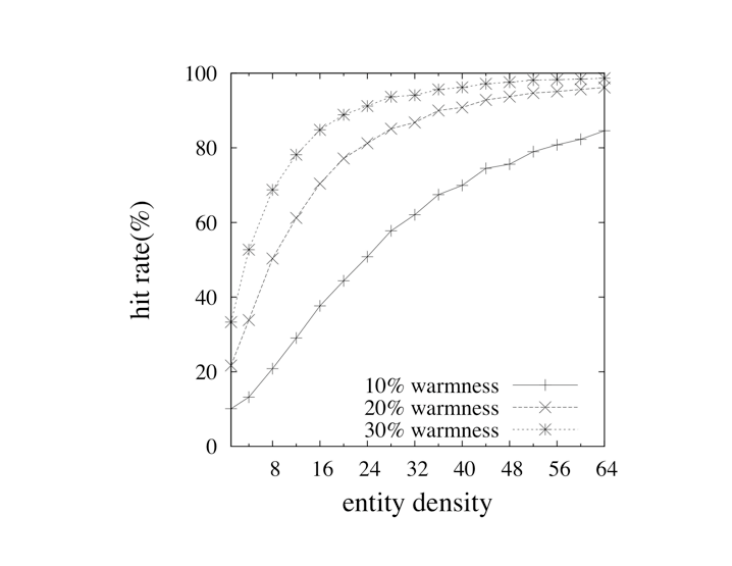
- SDP hit rate
  - a cache hit
    - a request is resolved by the SDP
  - higher hit rate => more requests resolved by the SDP
    - even when the PDP fails => higher availability
    - near the PEP => save latency

hit rate

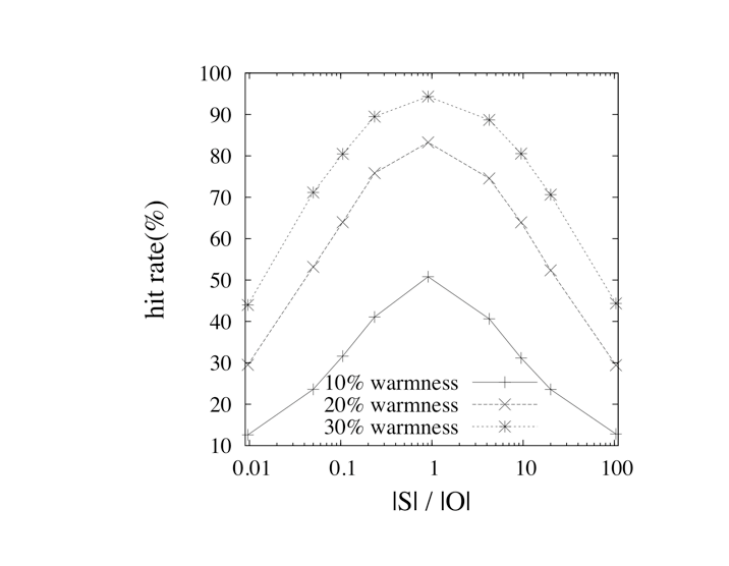
BLP policy: 5 levels, 5 categories, 50 subjects, 1,000 objects, 2 rights



impact of various system parameters

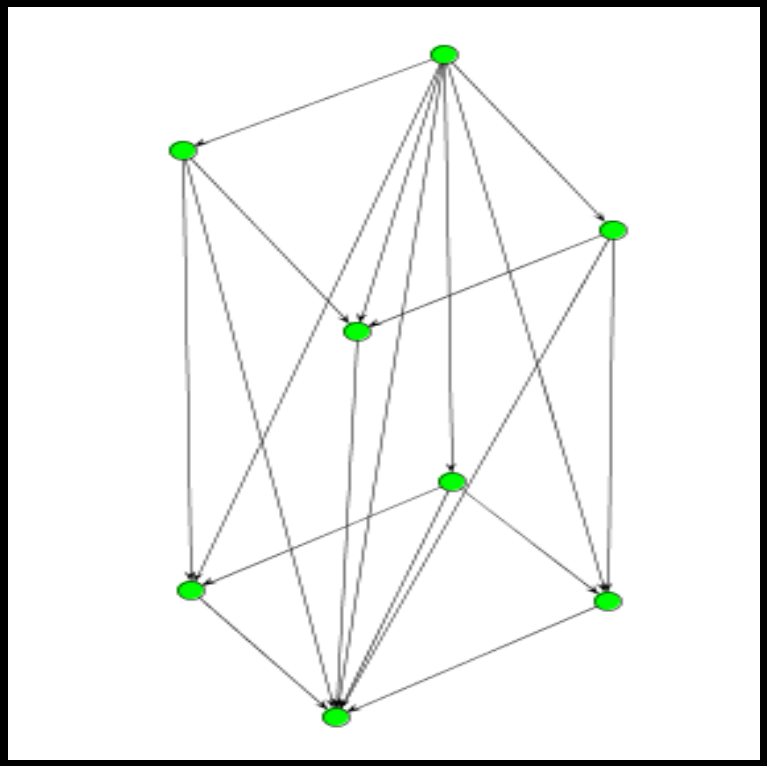


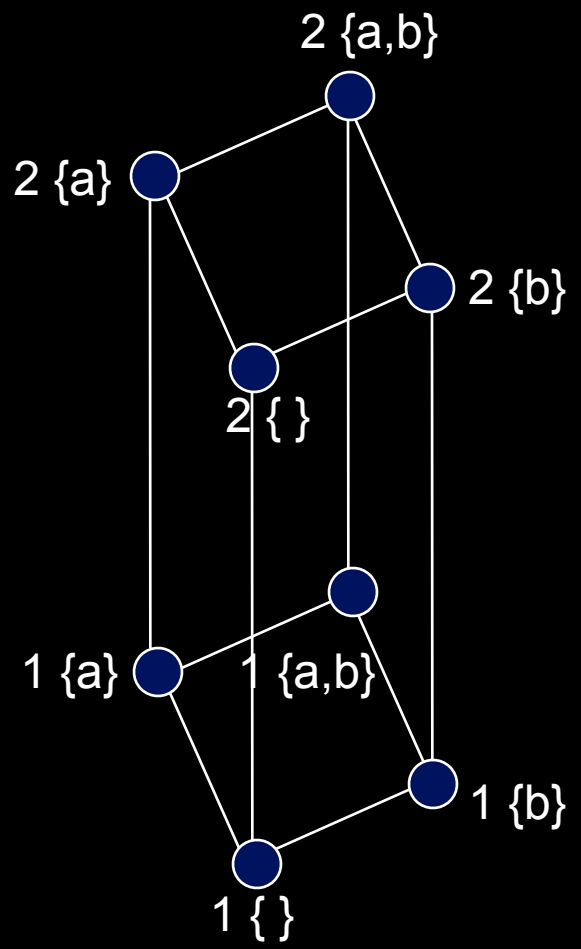
density of subjects and objects in the lattice



subject/object ratio

SDP DG and Security Lattice

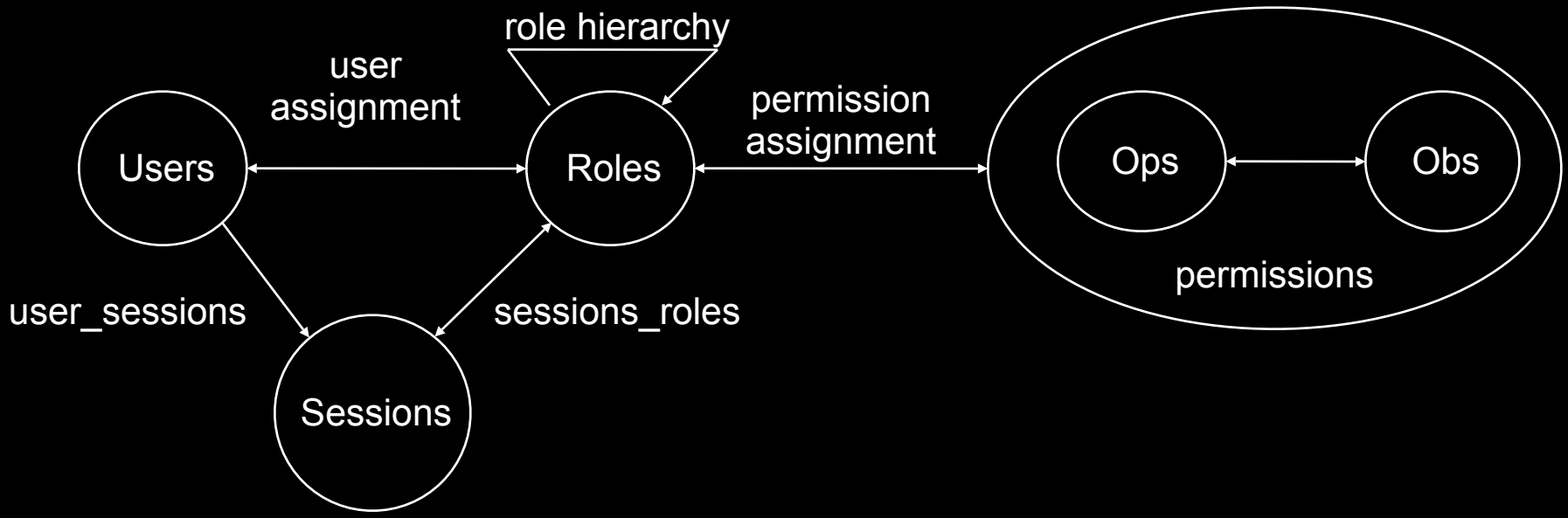




J. Crampton, W. Leung, K. Beznosov, "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies," in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Lake Tahoe, California, USA, 7-9 June, 2006, pp. 111-120.

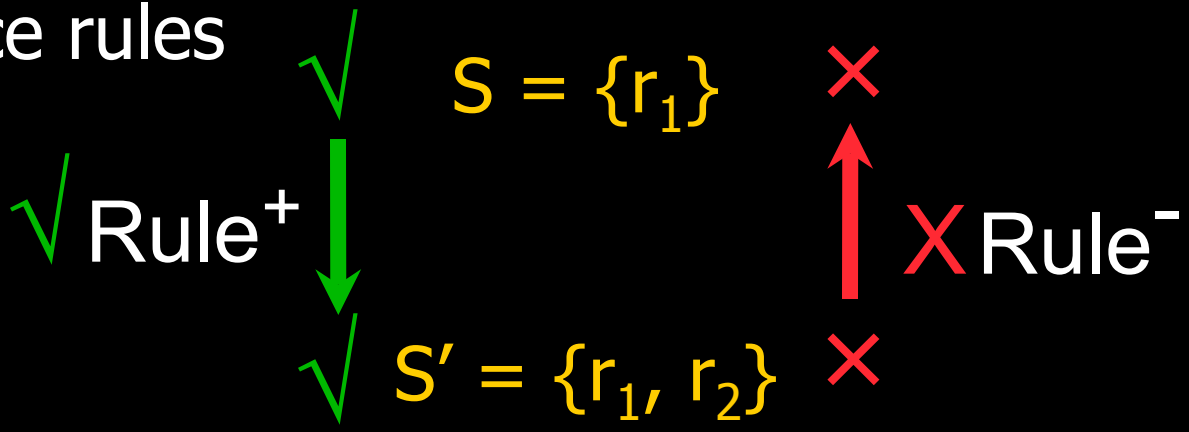
$SAAM_{RBAC}$: SAAM for RBAC

RBAC review

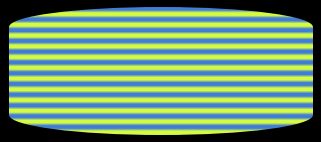

role hierarchy
user
assignment
permission
assignment
Users
Roles
Ops
Obs
permissions
user_sessions
sessions_roles
Sessions

preliminaries

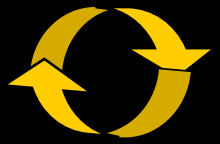
- request: issued by a subject for a permission.
  - request=(s,p)
- ±: denotes the decision to a request.
  - response=+(s,p) or –(s,p)
- subject: modeled as a set of roles.
  - s= $\{r_2, r_3, r_4\}$
- inference rules



recycling algorithms

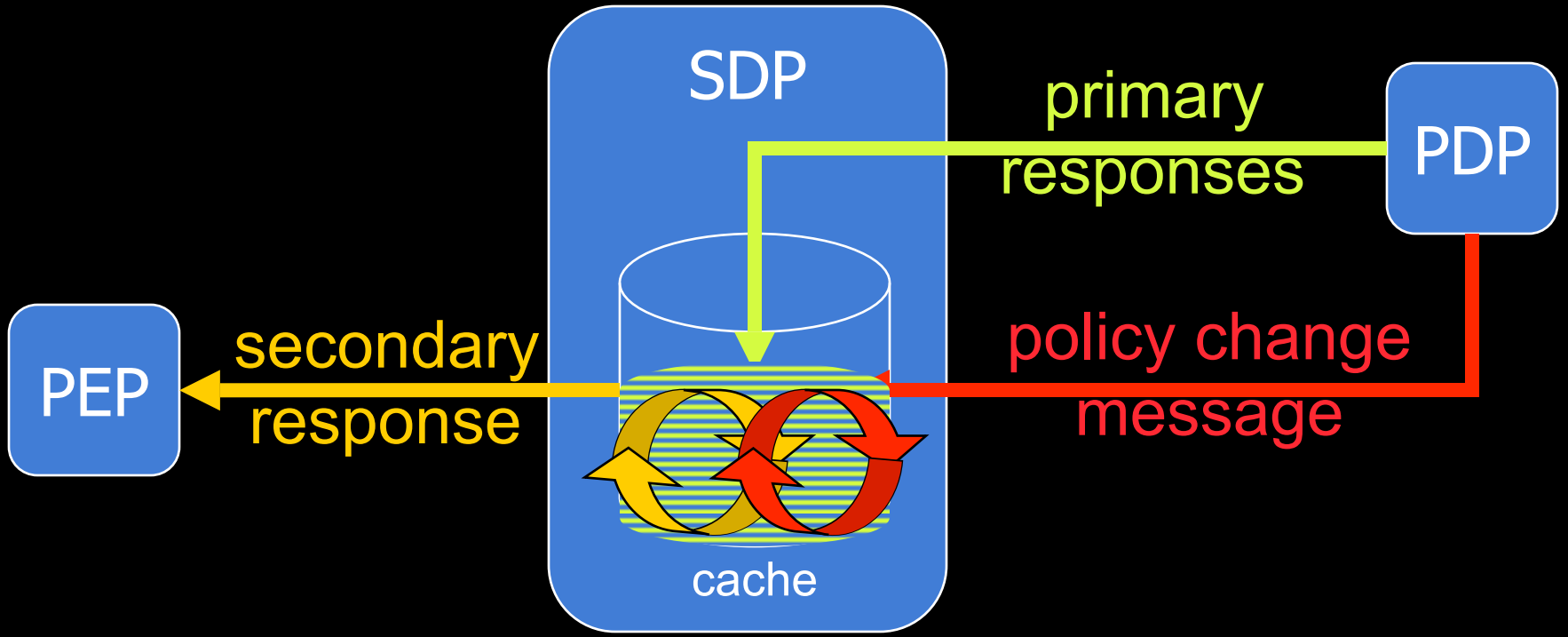


cache construction √



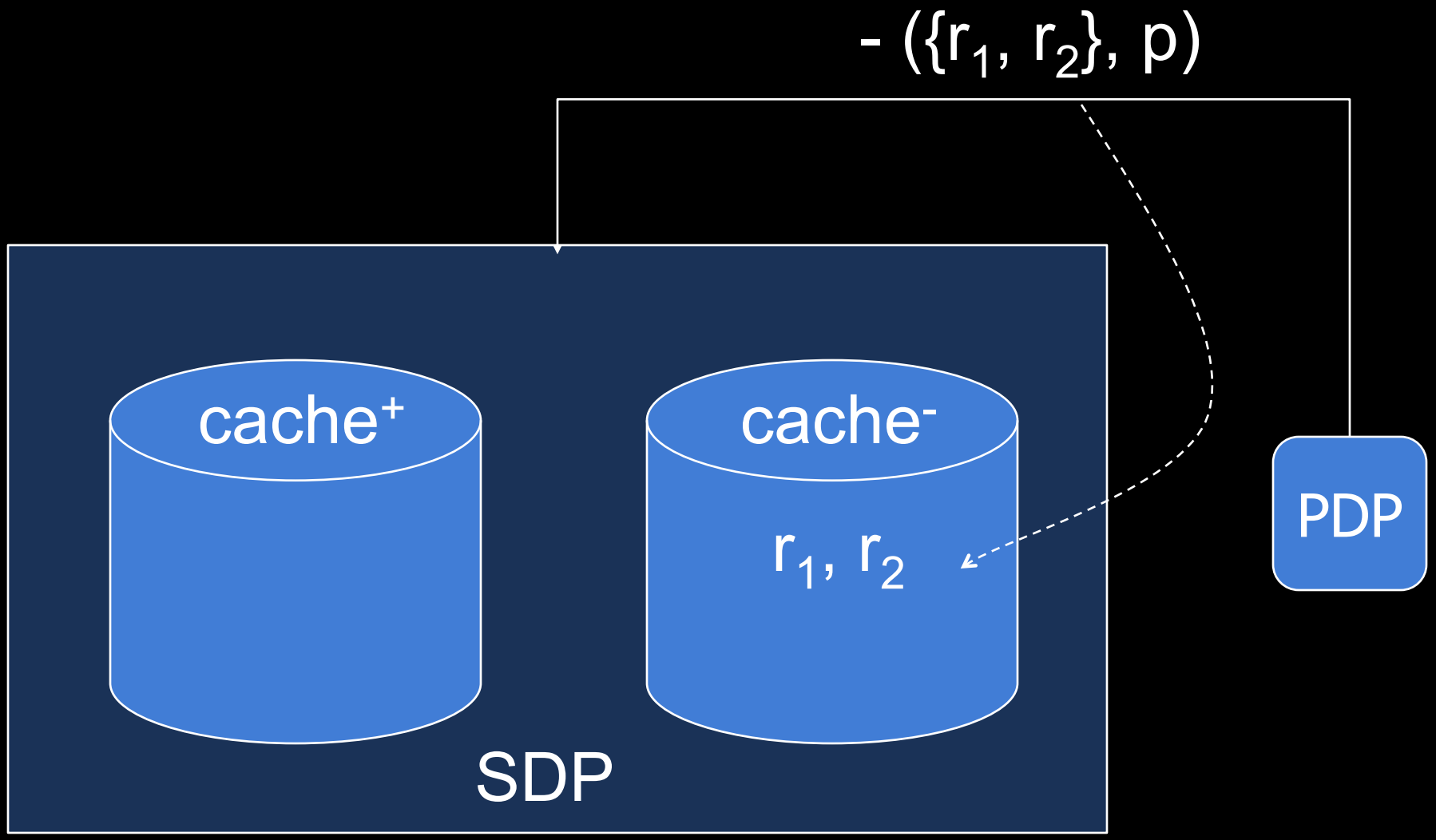
decision √

cache update

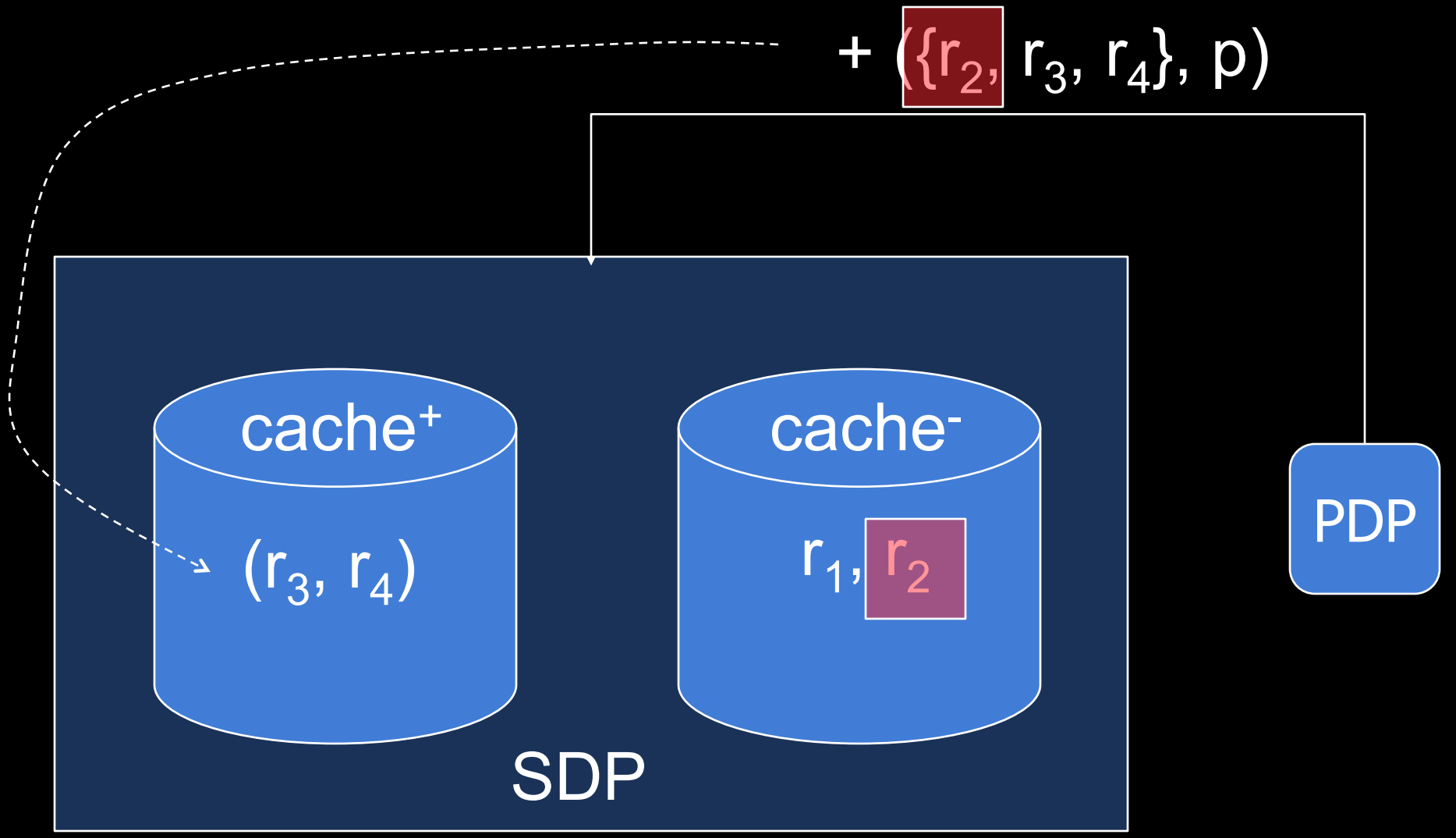


example

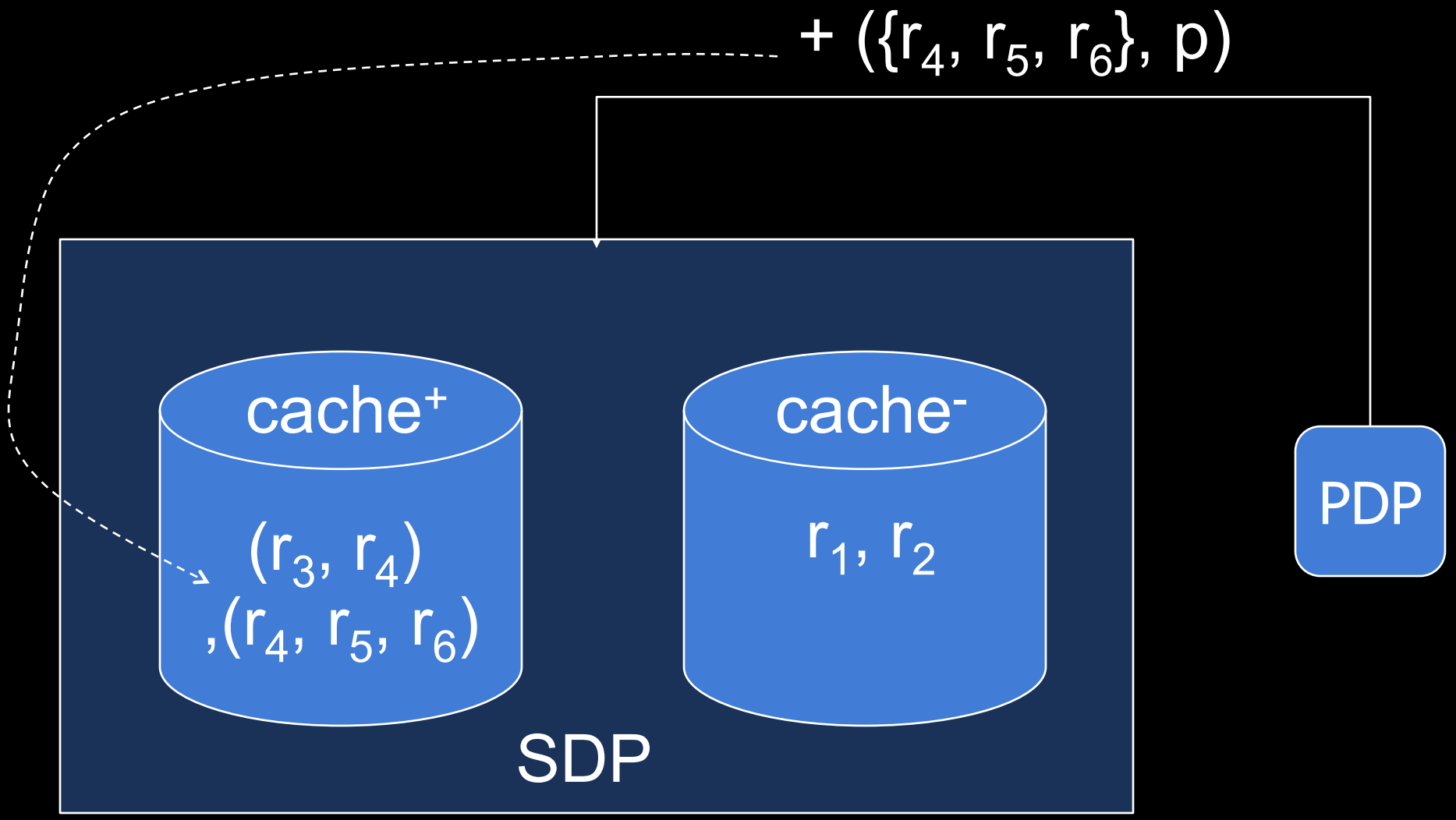
caching first negative decision



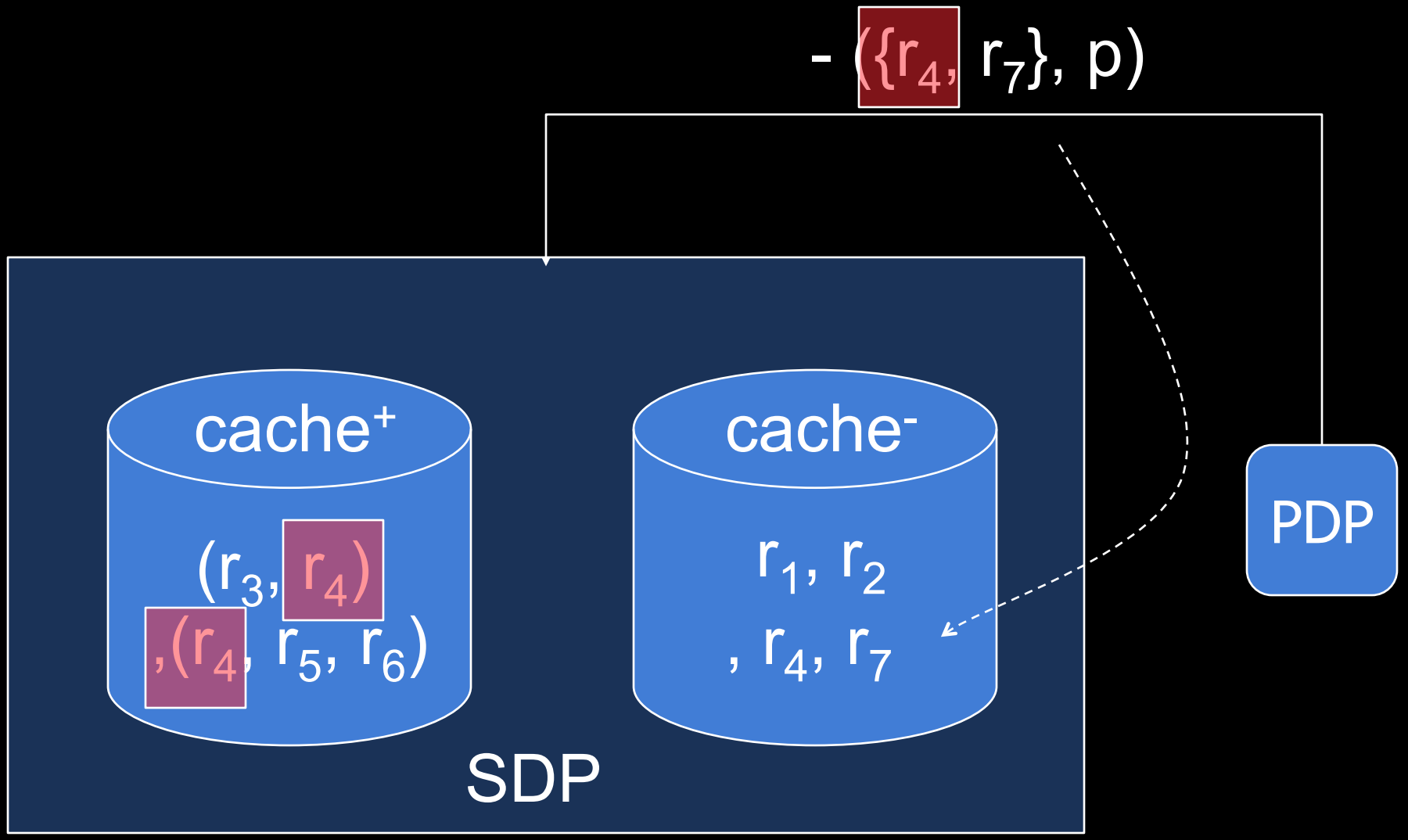
caching first positive decision



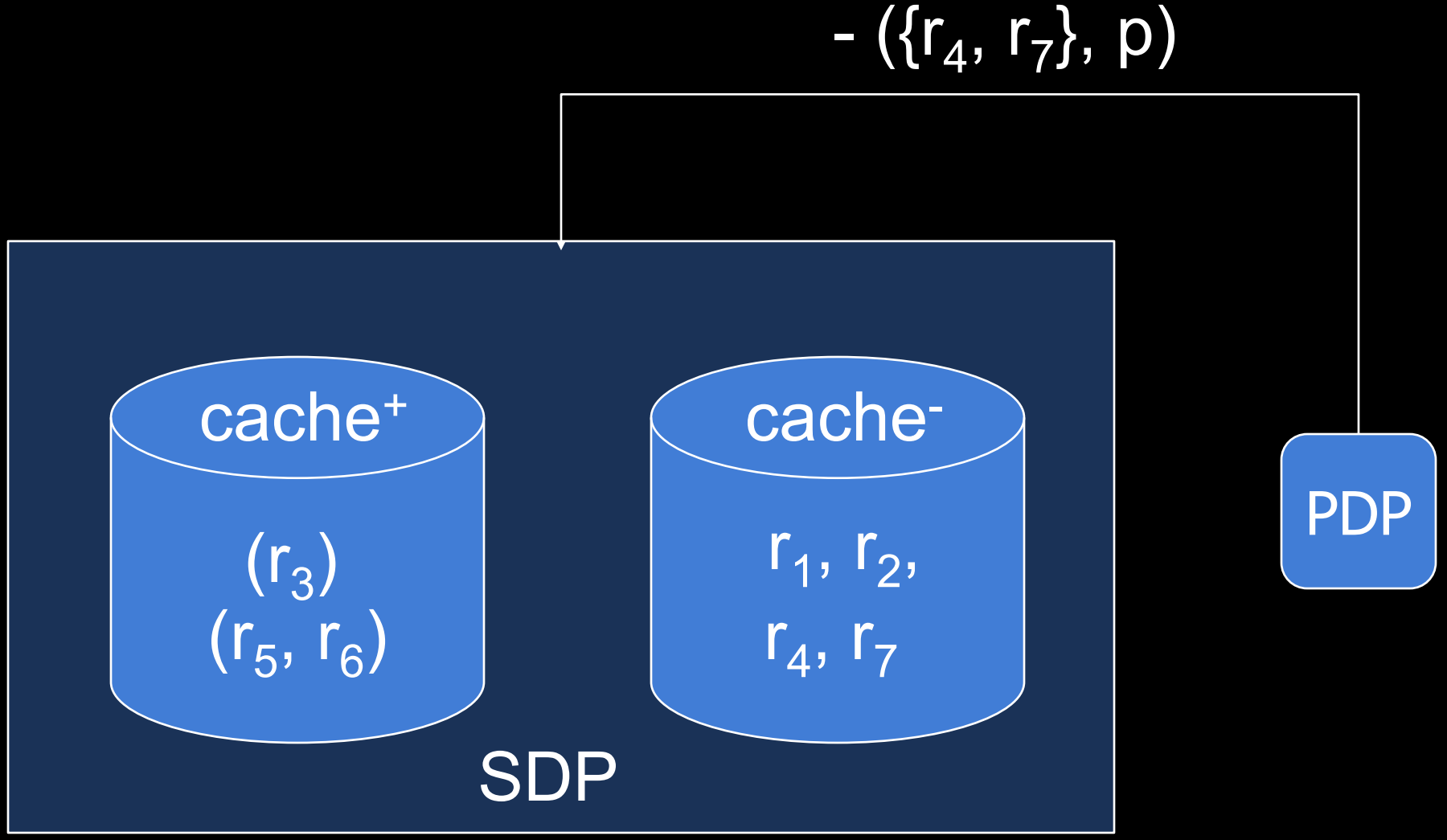
caching second positive decision



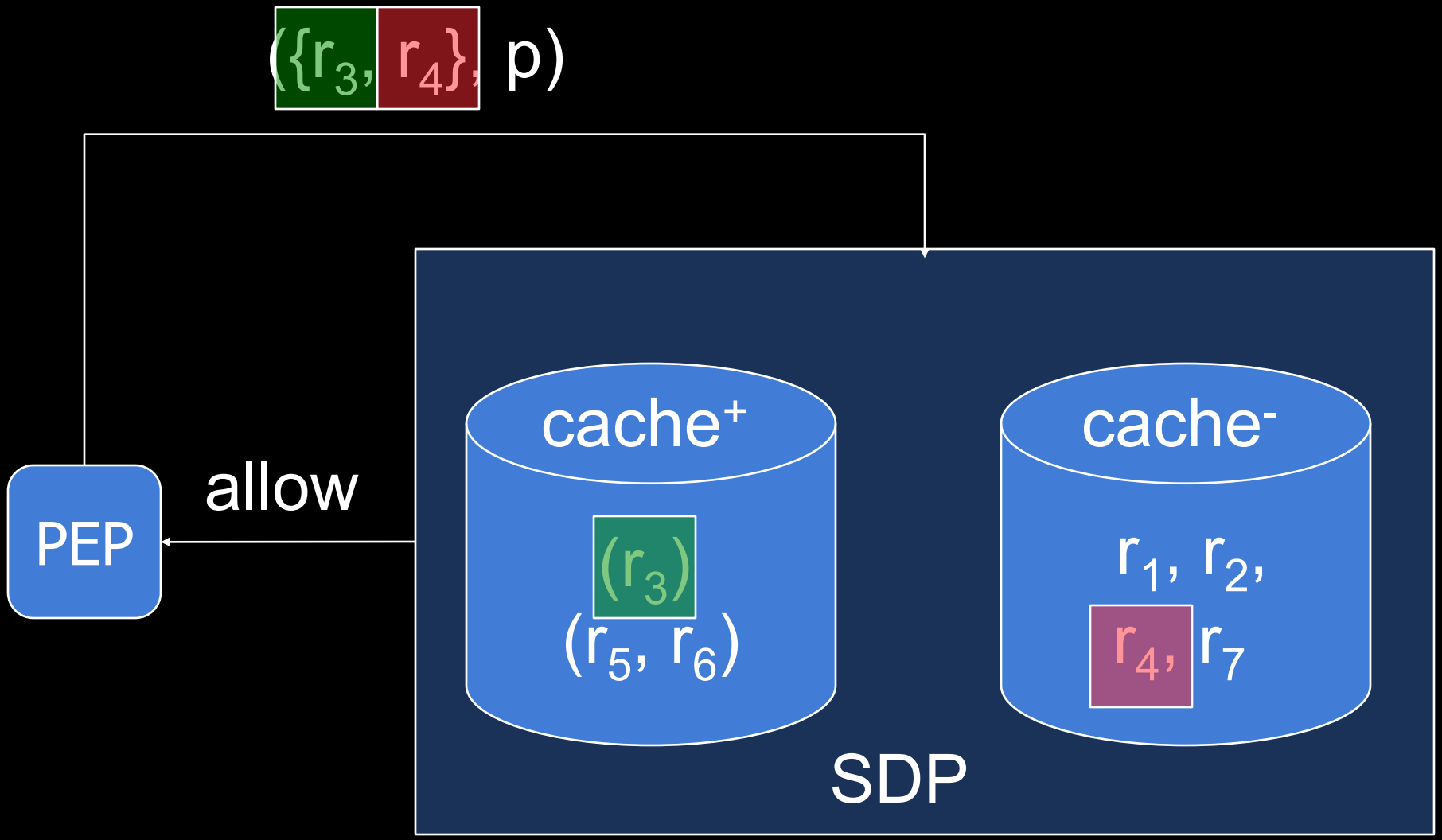
caching second negative decision



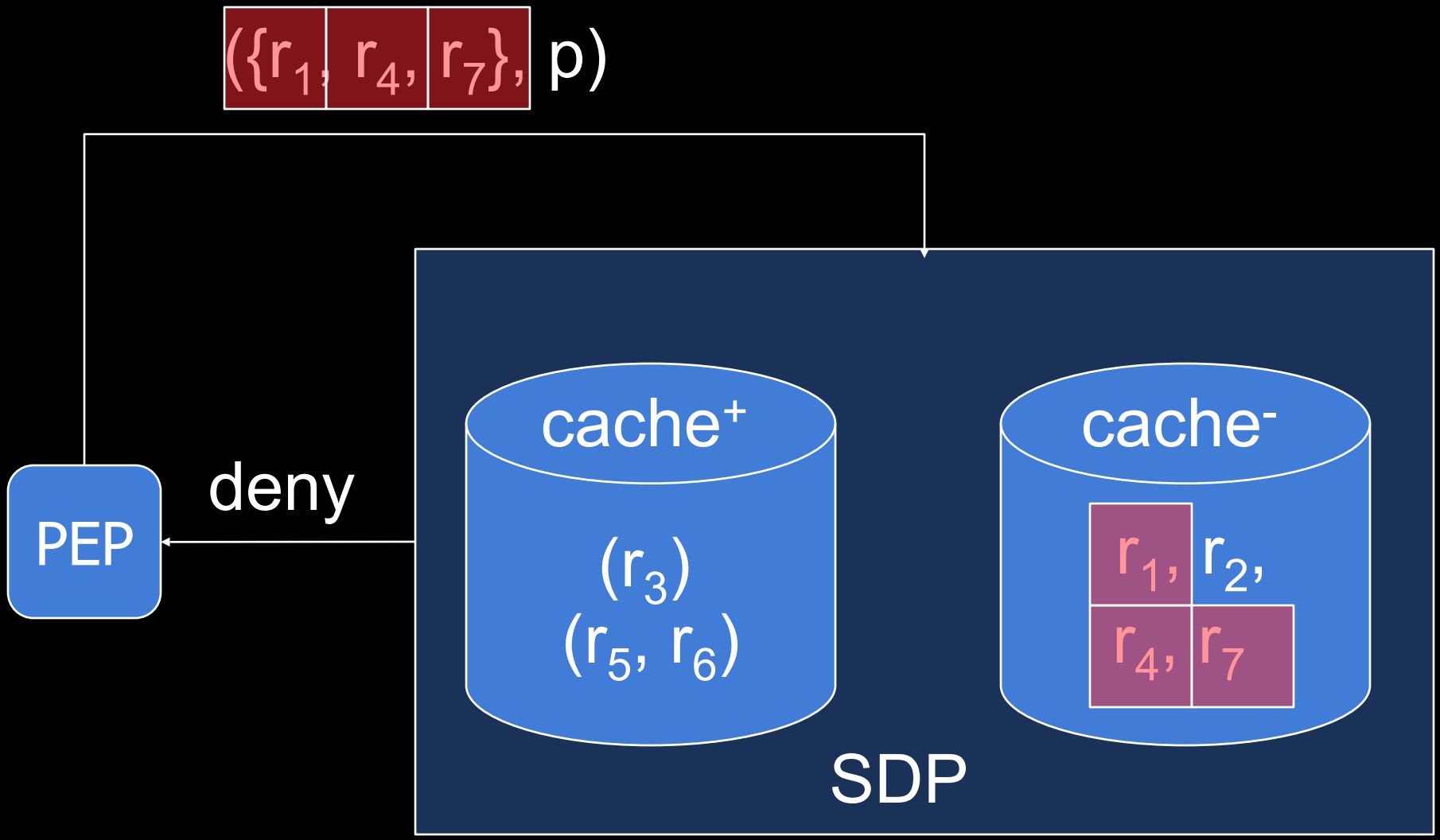
caching second negative decision



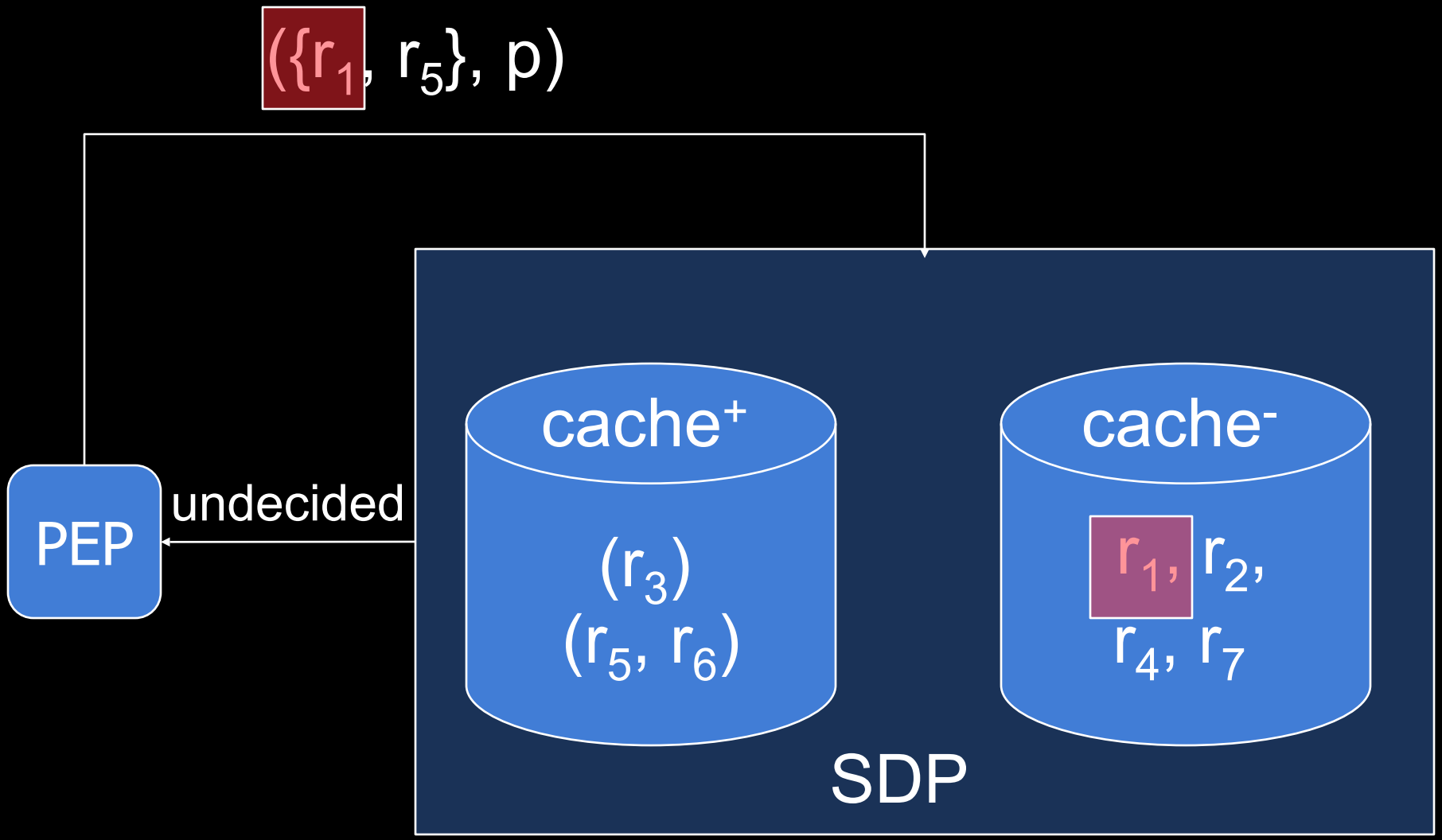
computing allowing authorization



computing denying authorization



computing undecided authorization

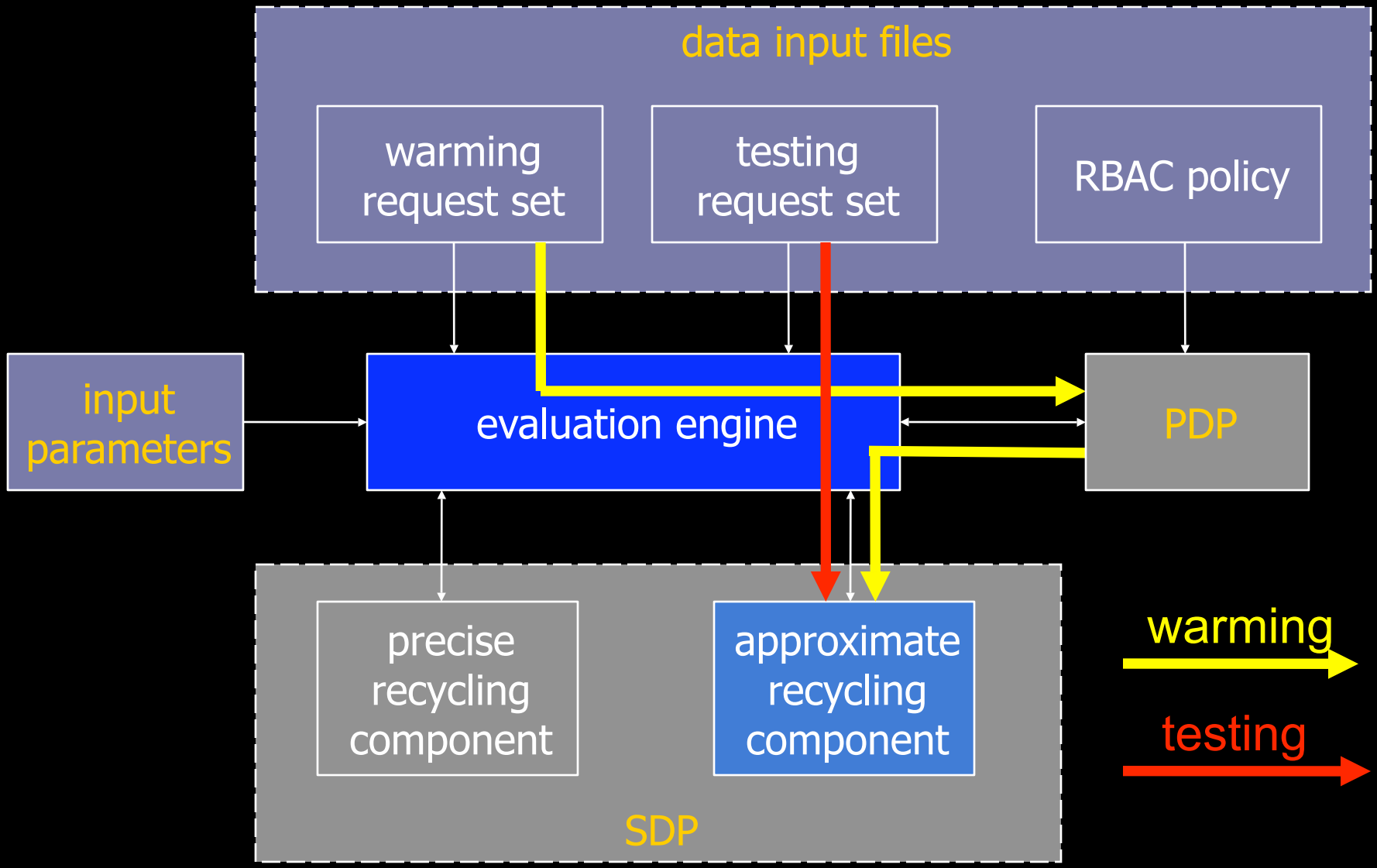


$SAAM_{RBAC}$ evaluation

evaluation metrics

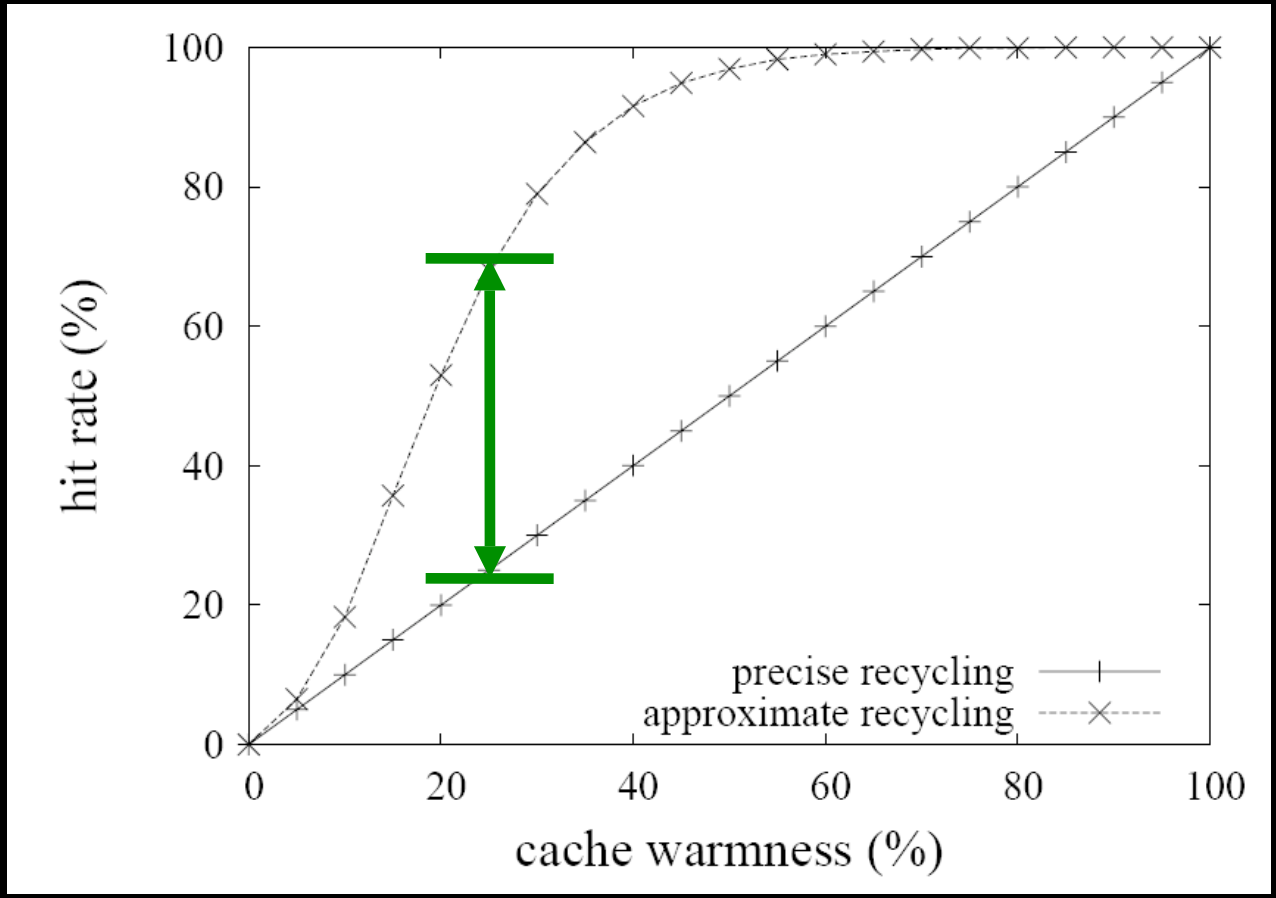
- SDP hit rate
- SDP inference time
  - the time used to infer approximate responses
  - less inference time, more efficient the system

evaluation methodology

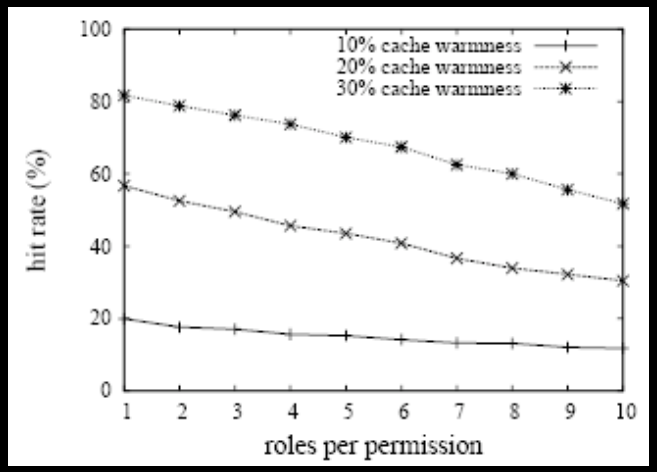


hit rate

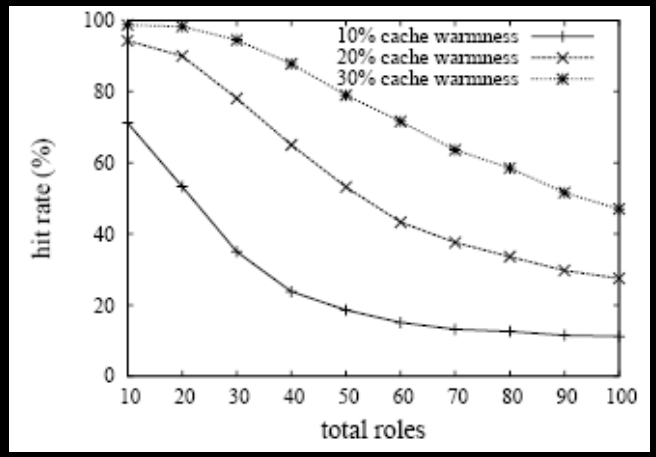
RBAC policy: 100 subjects, 1000 objects, 50 roles
uniform distribution



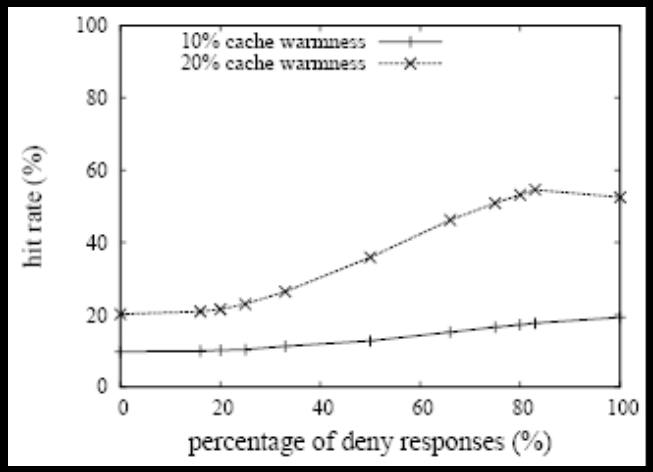
impact of various system parameters



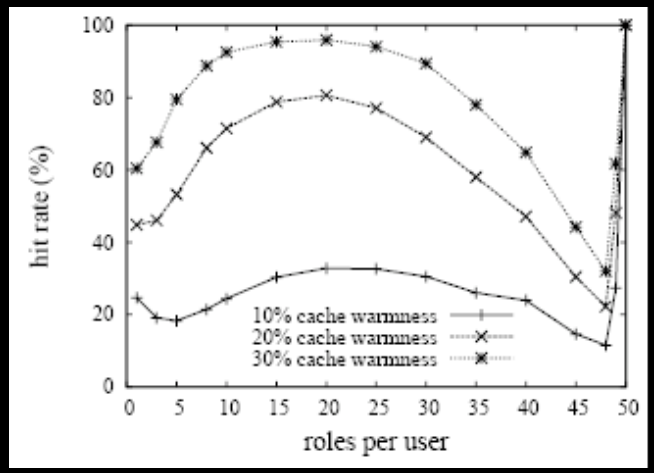
roles per permission



total roles

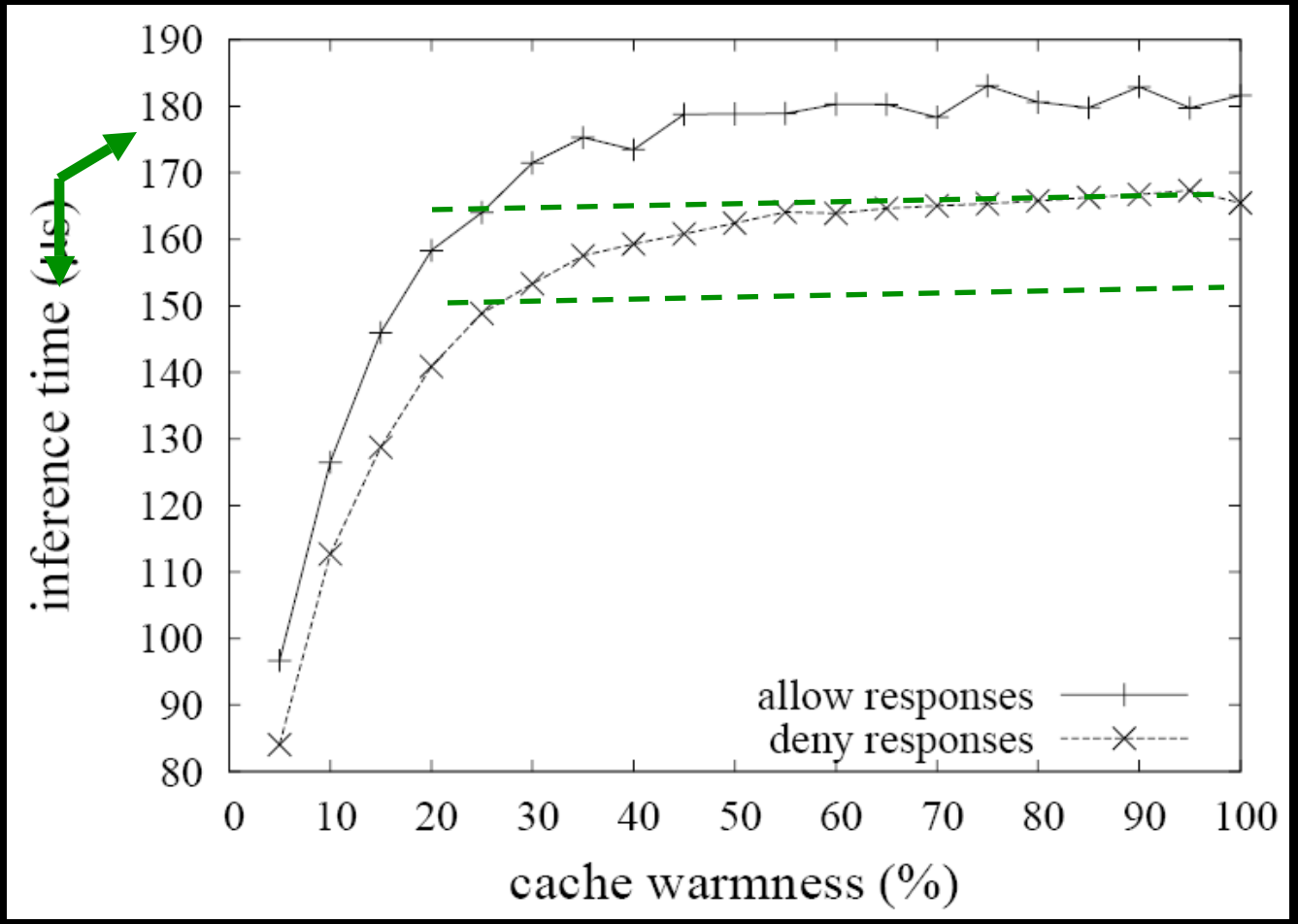


deny vs. allow responses



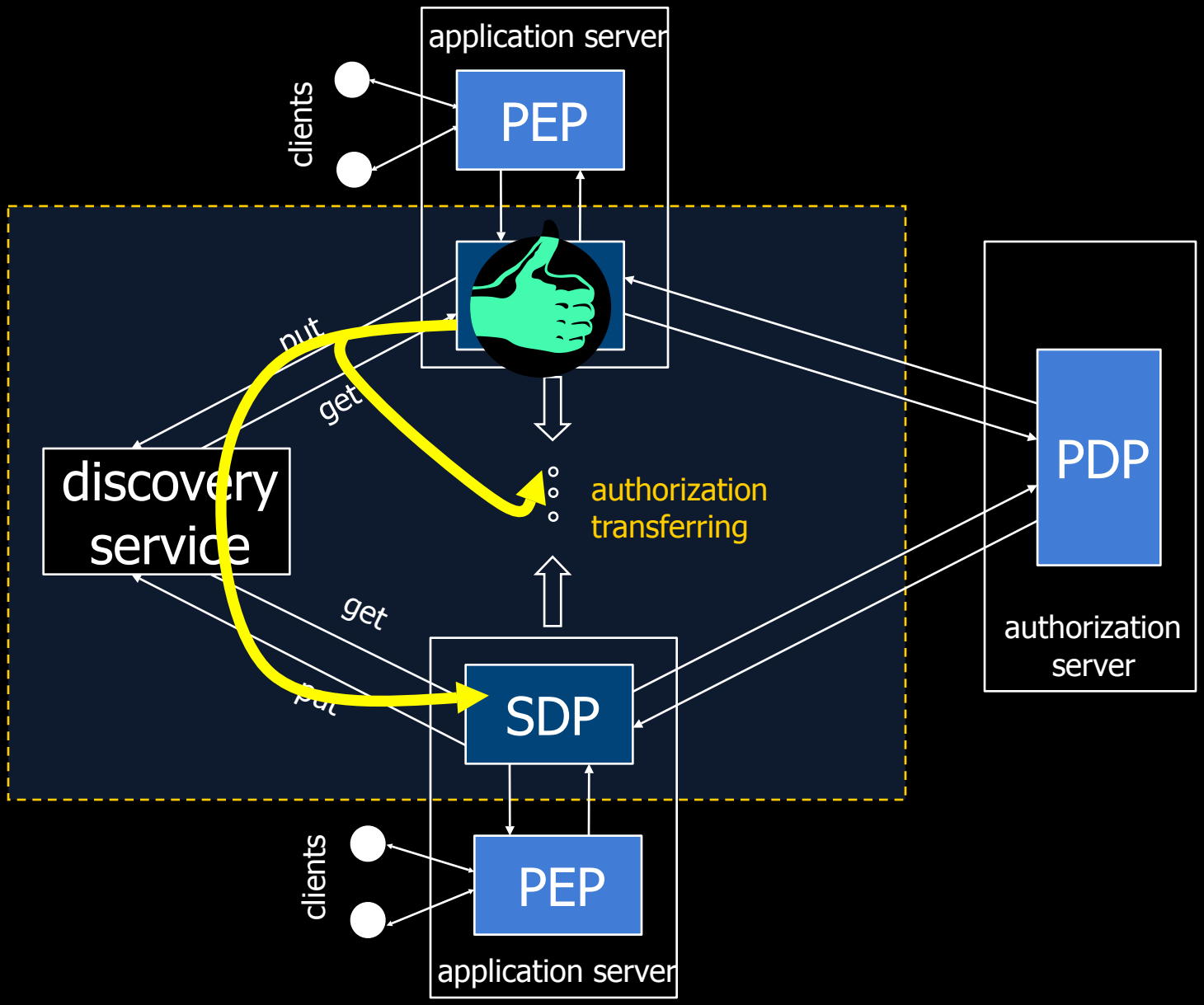
roles per user

inference time



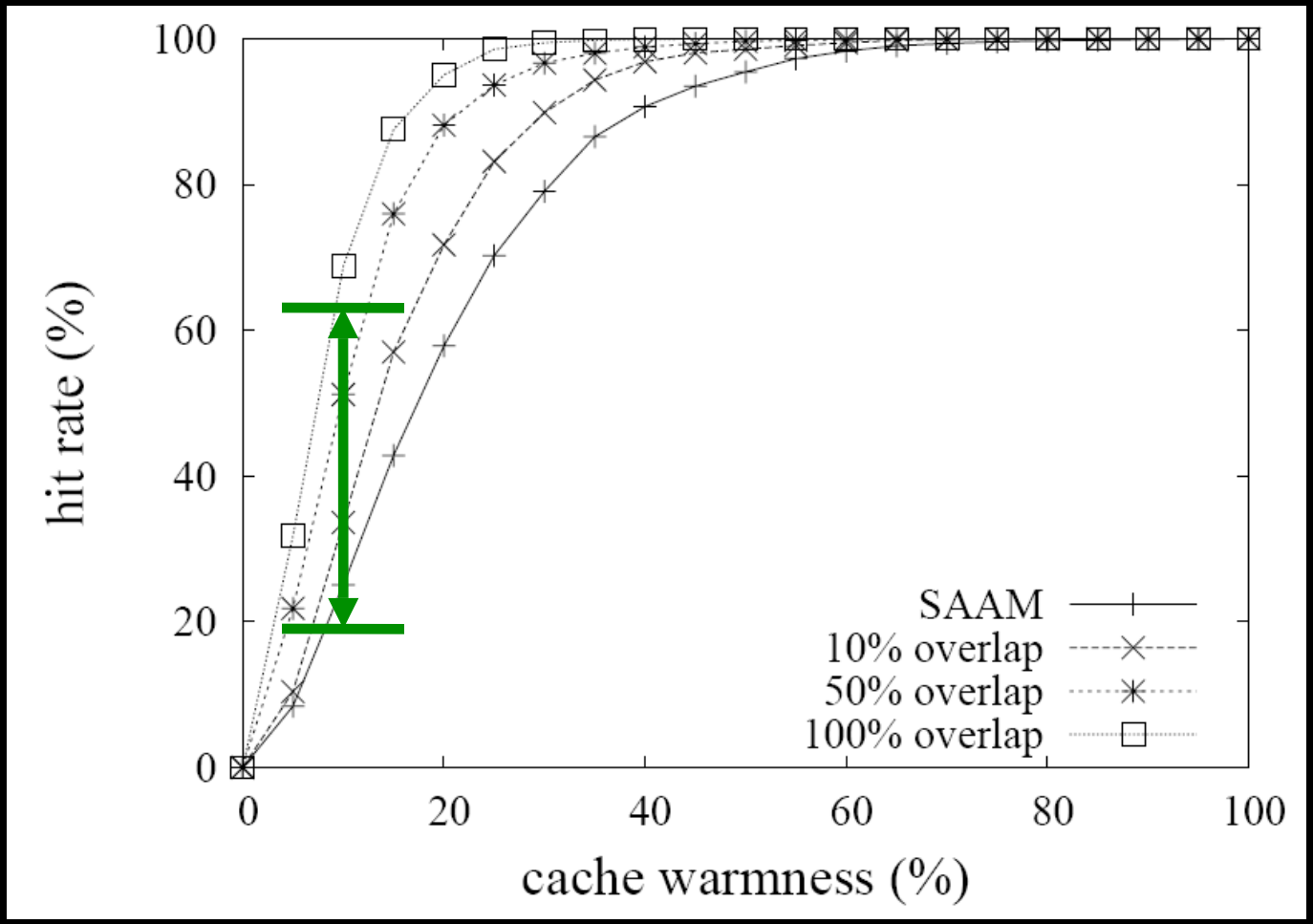
Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, "Authorization Recycling in RBAC Systems" to appear in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, 11-13 June 2008.

distributed and cooperative SAAM



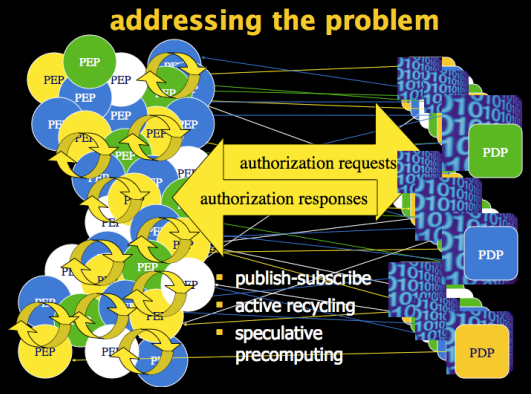
hit rate for distributed $SAAM_{BLP}$

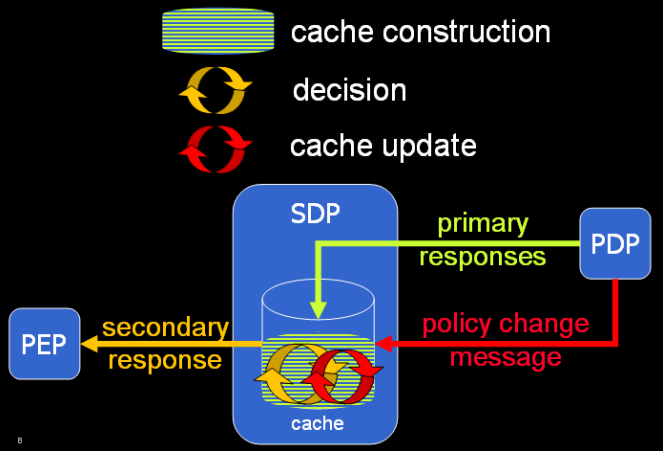
5 SDPs' cooperation, uniform requests

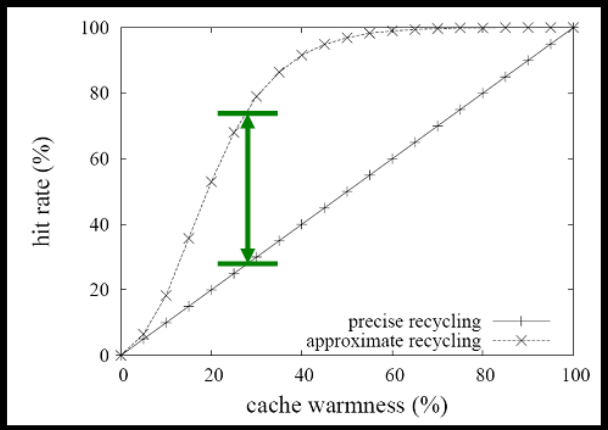


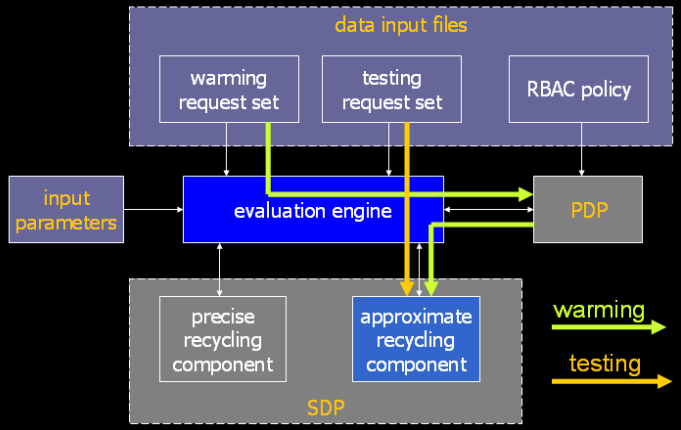
- Q. Wei, M. Repanu, K. Beznosov, "Cooperative Secondary and Approximate Authorization Recycling," in Proceedings of the IEEE International Symposium on High-Performance Distributed Computing (HPDC), Monterey Bay, CA, 27-29 June 2007, pp. 65-74.
- Q. Wei, M. Ripeanu, K. Beznosov, "Cooperative Secondary Authorization Recycling" 14 pages, to appear in the IEEE Transactions on Parallel and Distributed Systems.

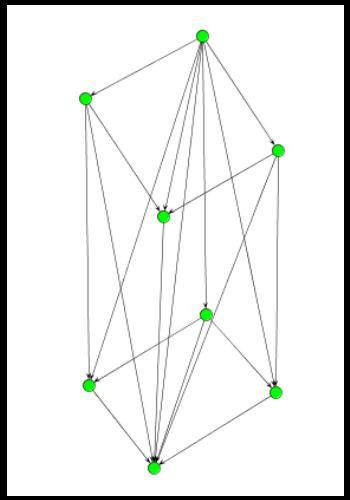
summary


addressing the problem
PEP
PDP
authorization requests
authorization responses
publish-subscribe
active recycling
speculative precomputing


cache construction
decision
cache update
SDP
primary responses
PDP
PEP
secondary response
policy change message
cache


hit rate (%)
cache warmness (%)
precise recycling
approximate recycling
0
20
40
60
80
100


data input files
warming request set
testing request set
RBAC policy
input parameters
evaluation engine
PDP
precise recycling component
approximate recycling component
SDP
warming
testing



project team

Qiang Wei

Wing Leung

Matei Ripeanu

Jason Crampton
Information Security
Group at Royal Holloway
University of London

Kosta Beznosov

summary

- secondary and approximate authorization model (SAAM)
  - secondary decision point (SDP)
  - classified response space
- SAAM algorithms for BLP and RBAC
- distributed and cooperative SAAM

selected project publications

- K. Beznosov, "Flooding and Recycling Authorizations" in Proceedings of New Security Paradigms Workshop (NSPW), 2005, Lake Arrowhead, CA, USA, 20-23 September 2005, pp. 67-72.
- SAAM for RBAC
  - Q. Wei, J. Crampton, K. Beznosov, M. Ripeanu, "Authorization Recycling in RBAC Systems" to appear in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Estes Park, Colorado, 11-13 June 2008.
- SAAM for Bell-Lapadula
  - J. Crampton, W. Leung, K. Beznosov, "The Secondary and Approximate Authorization Model and its Application to Bell-LaPadula Policies," in Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT), Lake Tahoe, California, USA, 7-9 June, 2006, pp. 111-120.
- Distributed and cooperative SAAM
  - Q. Wei, M. Repanu, K. Beznosov, "Cooperative Secondary and Approximate Authorization Recycling," in Proceedings of the IEEE International Symposium on High-Performance Distributed Computing (HPDC), Monterey Bay, CA, 27-29 June 2007, pp. 65-74.
  - Q. Wei, M. Ripeanu, K. Beznosov, "Cooperative Secondary Authorization Recycling" 14 pages, to appear in the IEEE Transactions on Parallel and Distributed Systems.

Konstantin (Kosta) Beznosov

konstantin.beznosov.net

supporting slides

Who's Konstantin Beznosov

- Education
  - M.S. (1997) & Ph.D. (2000) in CS, Florida International University
  - B.S. in Physics (1993), Novosibirsk State University
- Experience
  - Assistant Prof., Electr. and Comp. Egn., UBC (2003-present)
  - Directs Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
  - US industry (1997-2003): end-user, consulting, and software vendor organizations
- Contributed to
  - OMG
    - CORBA Security revisions
    - Resource Access Decision
    - Security Domain Membership Management
  - OASIS
    - eXtensible Access Control Markup Language (XACML) v1.0